Πανεπιστήμιο Πειραιώς

Τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων

Πρόγραμμα Μεταπτυχιακών Σπουδών

Ψηφιακές Επικοινωνίες και Δίκτυα

Διπλωματική Εργασία

ΜΕΛΕΤΗ ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ ΜΕ ΧΡΗΣΗ FIREWALL

Μάνος Ηλίας

Αθήνα 2008

Αφιερώνεται στους γονείς μου

Περίληψη

Η αυξανόμενη χρήση του διαδικτύου τόσο στην εργασία όσο και στα οικογενειακά περιβάλλοντα έχει αυξήσει την ευπάθεια των υπολογιστικών συστημάτων σε επιθέσεις από ένα μεγάλο εύρος απειλών. Η τεχνολογία των αντιπυρικών ζωνών συνεχίζει να είναι η πιο διαδεδομένη μορφή προστασίας, ενάντια στις υπάρχουσες και νέες απειλές στους υπολογιστές και τα δίκτυα. Η πλήρης κατανόηση των αντιπυρικών ζωνών, του τι μπορούν να πετύχουν, του τρόπου επέκτασης για την μέγιστη επίδραση, οι διαφορές μεταξύ των τύπων τους, αλλά και η κατάλληλη διαμόρφωση μπορούν να κάνουν τη διαφορά μεταξύ της ασφάλειας και της αποτυχίας στην προστασία των δικτύων.

Στην εργασία αυτή γίνεται μια προσπάθεια προσέγγισης στους διάφορους τύπους αντιπυρικών ζωνών, πρώτα εννοιολογικά και έπειτα εξηγώντας πώς οι διάφορες εφαρμογές αντιπυρικών ζωνών λειτουργούν σε πραγματικό περιβάλλον. Παρουσιάζονται επίσης πολλά παραδείγματα εφαρμογής, που δείχνουν τη χρήση των αντιπυρικών ζωνών σε απλά και σύνθετα σενάρια, επεξηγώντας τον τρόπο με τον όποιο πρέπει να εγκατασταθεί και να διαμορφωθεί μια αντιπυρική ζώνη. Επιπλέον, καθορίζονται και αναλύονται εντολές διαμόρφωσης και ανίχνευσης λαθών με σκοπό την σωστή διαμόρφωση και επίλυση των προβλημάτων που μπορεί να προκύψουν κατά την παραμετροποίηση των διαφορών τεχνολογιών.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον καθηγητή Δρ. Χρήστο Ξενάκη για την επίβλεψη και τη βοήθεια που μου παρείχε για την ολοκλήρωση της διπλωματικής μου.

Τέλος εκφράζω την ευγνωμοσύνη μου στους γονείς μου και την αδελφή μου για την υποστήριξη και βοήθειά τους σε όλη τη διάρκεια των μεταπτυχιακών σπουδών μου.

Περιεχόμενα

Κατάλογος πινάκων

Κατάλογος σχημάτων

Συντομογραφίες

AAA	Authentication Authorization Accounting
ABR	Area Border Router
ACE	Access Control Entry
ACL	Access Control Lists
AS	Autonomous System
ASBR	Autonomous System Boundary Router
ASDM	Adaptive Security Device Manager
BDR	Backup Designated Router
CA	Certification Authority
CLI	Command line interface
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DoS	Denial of Service
DR	Designated Router
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IPS	Intrusion Prevention System
IPSec	IP Security
IPv6	Internet Protocol version 6
ISAKMP	Internet Security Association and Key Management Protocol
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
NAS	Network Access Servers

NAT	Network Address Translation
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PAT	Port Address Translation
PKI	Public Key Infrastructure
PSK	Pre Shared Key
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RIP	Routing Information Protocol
SA	Security Associations
SMTP	Simple Mail Trnsfer Protocol
SNMP	Simple Network Management Protocol
SOHO	Small Office Home Office
SPF	Shortest Path First
SPI	Stateful Packet Inspection
SSH	Secure Shell
TACACS+	Terminal Access Controller Access Control System plus
TCP	Transmission Control Protocol
TSA	Totally stubby area
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VPN	Virtual Private Network

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Οι αντιπυρικές ζώνες αποτελούν ένα από τα βασικά συστατικά ενός ασφαλούς δικτύου. Η εργασία αυτή παρουσιάζει τις σύγχρονες δυνατότητες αντιπυρικών ζωνών και τον τρόπο διαμόρφωσής τους, ωστόσο δεν αποτελεί μια λεπτομερή αναφορά σε όλες τις πιθανές αντιπυρικές ζώνες. Σκοπός της είναι να αποτελέσει τη βάση στην οποία θα οικοδομηθούν η γνώση και οι δεξιότητες στη διαχείριση και την ανάπτυξη αντιπυρικών ζωνών, αλλά και της ασφάλειας γενικότερα. Αν και τα προϊόντα αντιπυρικών ζωνών ποικίλλουν, οι θεμελιώδεις αρχές της τεχνολογίας δεν διαφέρουν. Από την σκοπιά της διαμόρφωσης η παρούσα εργασία εστιάζει στις συσκευές ασφάλειας Cisco PIX και ASA.

Η εργασία δομείται σε κεφάλαια ως εξής: Τα κεφάλαια 2 έως 4 παρέχουν το απαραίτητο θεωρητικό υπόβαθρο στις αντιπυρικές ζώνες. Επικεντρώνονται στην ταξινόμηση, τις τεχνολογίες και αρχιτεκτονικές που αφορούν τις αντιπυρικές ζώνες. Τα κεφάλαια 5 έως 7 περιγράφουν την πρόσβαση και διαμόρφωση των βασικών τεχνολογιών στις αντιπυρικές ζώνες PIX και ASA. Η ανάπτυξη και διαμόρφωση περισσότερο συνθέτων και ειδικών σεναρίων (AAA, OSPF, VPN) παρουσιάζεται στα κεφάλαια 8 έως 10. Στο κεφάλαιο 11 παρουσιάζονται τα συμπεράσματα και προτάσεις για μελλοντική εργασία. Ακολουθεί μια γρήγορη επισκόπηση του περιεχομένου για τα διάφορα κεφάλαια:

Κεφάλαιο 2, "Εισαγωγή στις αντιπυρικές ζώνες". Αποτελεί την εισαγωγή στις αντιπυρικές ζώνες και το τι μπορούν να κάνουν. Εστιάζει στο τι είναι μια αντιπυρική ζώνη, ποιες απειλές ασφάλειας υπάρχουν, τι είναι η πολιτική ασφάλειας αντιπυρικών ζωνών και πώς μπορούμε να χρησιμοποιήσουμε την αντιπυρική ζώνη για προστασία από απειλές.

Κεφάλαιο 3, "Ταξινόμηση αντιπυρικών ζωνών". Αυτό το κεφάλαιο καλύπτει τις διαφορές τεχνολογιών αντιπυρικών ζωνών. Εξετάζει τη βασική ταξινόμηση των αντιπυρικών ζωνών σε αντιπυρικές ζώνες για προσωπικούς υπολογιστές,

μικρούς και μεγάλους οργανισμούς. Επιπλέον, αναλύει τους τρόπους που οι αντιπυρικές ζώνες υπερασπίζονται τα δίκτυα, από τα απλά και αναλυτικά φίλτρα πακέτων έως τα πληρεξούσια εφαρμογής. Παρέχει επίσης και μια επισκόπηση των διάφορων προϊόντων αντιπυρικών ζωνών.

Κεφάλαιο 4, "Τοπολογίες και αρχιτεκτονικές αντιπυρικών ζωνών". Το κεφάλαιο αυτό ασχολείται με το σχεδιασμό της ανάπτυξης των αντιπυρικών ζωνών. Γίνεται ανάλυση των διαφορετικών αρχιτεκτονικών αντιπυρικών, συμπεριλαμβανομένης της διπλής αντιπυρικής ζώνης και των διαφορετικών τύπων εφαρμογών DMZ. Αυτό το κεφάλαιο ερευνά επίσης τους διαφορετικούς τύπους αντιπυρικών ζωνών και τα αντίστοιχα σημεία εγκατάστασης στο δίκτυο για μέγιστη αποτελεσματικότητα.

Κεφάλαιο 5, "Βασική διαμόρφωση αντιπυρικής ζώνης". Σκοπός αυτού του κεφαλαίου είναι να κάνει μια εισαγωγή στη διαμόρφωση των συσκευών ασφάλειας PIX και ASA. Το κεφαλαίο αρχίζει με την περιγραφή του τρόπου πρόσβασης και στη συνεχεία παρουσιάζει τις βασικές εντολές που απαιτούνται για την βασική διαμόρφωση και παρακολούθηση.

Κεφάλαιο 6, "Μεταφράσεις και συνδέσεις". Αυτό το κεφαλαίο αναφέρεται στις μεταφράσεις και συνδέσεις των συσκευών ασφάλειας. Πρώτα, αναλύεται ο τρόπος που οι συσκευές ασφάλειας επεξεργάζονται την κυκλοφορία TCP και UDP. Στη συνεχεία μελετάται η διαμόρφωση των συσκευών ασφάλειας για να υποστηρίξουν τις δυναμικές και στατικές μεταφράσεις διευθύνσεων.

Κεφάλαιο 7, "Κατάλογοι ελέγχου πρόσβασης". Συζητά τον τρόπο που οι συσκευές ασφάλειας χρησιμοποιούν τους καταλόγους ελέγχου πρόσβασης (ACL) για τον έλεγχο της κυκλοφορίας. Παρουσιάζεται η θεωρία και ο τρόπος λειτουργίας των ACL μαζί με λεπτομερή παραδείγματα ειδικών σεναρίων.

Κεφάλαιο 8, "Επικύρωση - Έγκριση - Παρακολούθηση". Οι συσκευές ασφάλειας χρησιμοποιούν την επικύρωση, την έγκριση και την παρακολούθηση (AAA) για να εκτελέσουν τις λειτουργίες της πιστοποίησης ταυτότητας, την παροχή πρόσβασης και την παρακολούθηση των κινήσεων του χρήστη. Αυτό το

κεφάλαιο παρέχει τον τρόπο διαμόρφωσης για τις υπηρεσίες AAA με τον καθορισμό ενός καταλόγου μεθόδων επικύρωσης για τις διάφορες υλοποιήσεις.

Κεφάλαιο 9, "Δρομολόγηση". Στο παρόν κεφάλαιο περιλαμβάνονται οι ικανότητες δρομολόγησης των συσκευών ασφάλειας. Πρώτα αναλύεται η στατική δρομολόγηση και στη συνεχεία τα πρωτοκόλλα RIP και OSPF, σε συνδυασμό με την αντίστοιχη υλοποίηση.

Κεφάλαιο 10, "Intranet VPN". Η υποστήριξη δυνατοτήτων IPSec VPN από τις αντιπυρικές ζώνες, μας επιτρέπει να συνδέσουμε δίκτυα που είναι τοποθετημένα σε διαφορετικές γεωγραφικές θέσεις. Το κεφάλαιο παρέχει τις μεθόδους διαμόρφωσης και ανίχνευσης λαθών, ώστε να υλοποιηθεί με επιτυχία ένα Intranet IPSec VPN.

Κεφάλαιο 11, "Συμπεράσματα". Στο τελευταίο κεφάλαιο παρουσιάζονται τα συμπεράσματα και προτάσεις για μελλοντική εργασία.

ΚΕΦΑΛΑΙΟ 2

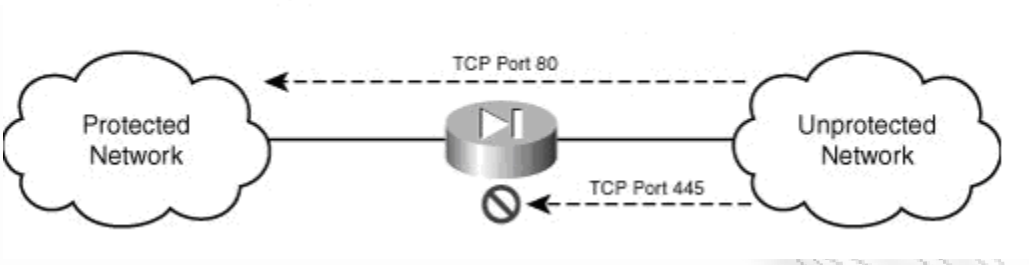
Εισαγωγή στις αντιπυρικές ζώνες

2.1 Εισαγωγή

Μια αντιπυρική ζώνη (firewall) μπορεί να γίνει είτε ο ακρογωνιαίος λίθος της υποδομής ασφάλειας ενός οργανισμού, είτε μια συσκευή που θα έχει αποτύχει να αντεπεξέλθει στις προσδοκίες μας. Ο μεγαλύτερος λόγος της αποτυχίας είναι η παρανόηση για αυτό που μια αντιπυρική ζώνη είναι, ή δεν είναι, και τι μπορεί, ή δεν μπορεί, να κάνει. Αυτό το κεφάλαιο εξετάζει τι είναι μια αντιπυρική ζώνη και πώς λειτουργεί, ώστε να επεξηγήσει τις λογικές προσδοκίες από μια αντιπυρική ζώνη. Εξετάζει επίσης τις απειλές που υπάρχουν και τα κίνητρα των επιτιθεμένων, για να δείξει το πώς οι αντιπυρικές ζώνες μπορούν ή όχι να προστατεύσουν από τις αντίστοιχες επιθέσεις.

2.2 Τι είναι μια αντιπυρική ζώνη;

Όταν οι περισσότεροι άνθρωποι ακούσουν τον όρο firewall, σκέφτονται μια συσκευή που υπάρχει στο δίκτυο και ελέγχει τα δεδομένα που περνούν από ένα δίκτυο υπολογιστών σε ένα άλλο, όπως η αντιπυρική ζώνη στο σχήμα 2-1 (network-based firewall). Ωστόσο, οι αντιπυρικές ζώνες μπορούν επίσης να εφαρμοστούν και στα ίδια τα συστήματα υπολογιστών, όπως το Microsoft Internet Connection Firewall (ICF). Σε αυτή την περίπτωση είναι γνωστές ως host-based firewalls. Και οι δύο τύποι αντιπυρικών ζωνών έχουν τον ίδιο στόχο: Να παρέχουν μια μέθοδο που θα ενισχύει την πολιτική ελέγχου πρόσβασης. Στον απλούστερο ορισμό, οι αντιπυρικές ζώνες δεν είναι τίποτα περισσότερο από σημεία επιβολής πολιτικής ελέγχου πρόσβασης.



Σχήμα 2-1 : Αντιπυρική ζώνη δικτύων

Οι αντιπυρικές ζώνες μας επιτρέπουν να καθορίσουμε μια απαίτηση ελέγχου πρόσβασης και να εξασφαλίσουμε ότι μόνο η κίνηση (traffic) που πληρεί την απαίτηση μπορεί να διαπεράσει την αντιπυρική ζώνη (στην περίπτωση ενός network-based firewall) ή να έχει πρόσβαση στο προστατευμένο σύστημα (στην περίπτωση του host-based firewall). Το σχήμα 2-1 δείχνει τον τρόπο που χρησιμοποιήσουμε μια network-based αντιπυρική ζώνη για να επιτρέψουμε μόνο σε συγκεκριμένη κίνηση να έχει πρόσβαση στους προστατευμένος πόρους.

2.3 Τι μπορούν να κάνουν οι αντιπυρικές ζώνες;

Όλες οι αντιπυρικές ζώνες μοιράζονται μερικά κοινά γνωρίσματα και λειτουργίες που καθορίζουν τι μπορεί μια αντιπυρική ζώνη να κάνει. Οι αντιπυρικές ζώνες πρέπει να είναι σε θέση να εκτελέσουν τις ακόλουθους εργασίες:

1. Διαχείριση και έλεγχο την κίνησης στο δίκτυο
2. Επικύρωση πρόσβασης
3. Λειτουργία μεσολαβητή
4. Προστασία πόρων
5. Καταγραφή και αναφορά συμβάντων

2.3.1 Διαχείριση και έλεγχος την κίνησης στο δίκτυο

Η πρώτη και θεμελιώδης λειτουργία που όλες οι αντιπυρικές ζώνες πρέπει να εκτελέσουν είναι να διαχειρίζονται και να ελέγχουν την κίνηση που επιτρέπεται να έχει πρόσβαση στο προστατευμένο δίκτυο ή υπολογιστή. Οι αντιπυρικές ζώνες το επιτυγχάνουν αυτό με την επιθεώρηση των πακέτων και των έλεγχο των συνδέσεων που πραγματοποιούνται. Φιλτράρουν τις συνδέσεις συμφώνα με τα αποτελέσματα της επιθεώρησης πακέτων (packet-inspection) και των συνδέσεων.

Επιθεώρηση πακέτων: Είναι η διαδικασία της επεξεργασίας των δεδομένων σε ένα πακέτο με στόχο να καθορίσει εάν πρέπει να επιτραπεί ή απαγορευτεί σύμφωνα με την προκαθορισμένη πολιτική πρόσβασης. Η επιθεώρηση πακέτων μπορεί να εξετάσει ένα ή όλα τα ακόλουθα στοιχεία:

- IP διεύθυνση πηγής (Source IP address)
- Θύρα πηγής (Source port)
- IP διεύθυνση προορισμού (Destination IP address)
- Θύρα προορισμού (Destination port)
- IP πρωτόκολλο (IP protocol)
- Πληροφορίες επικεφαλίδας πακέτων (Packet header information)

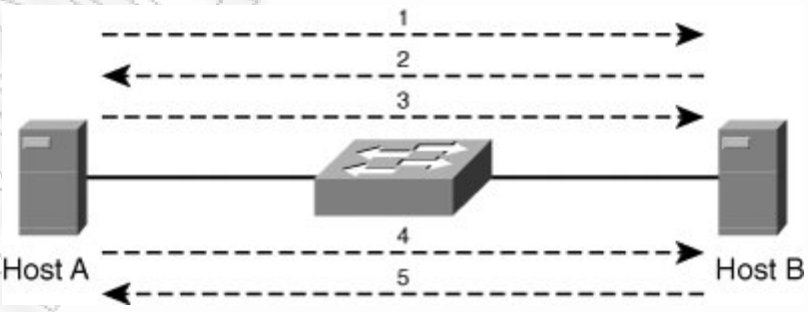
Ένα σημαντικό γεγονός που θα πρέπει να λάβουμε υπόψη για την επιθεώρηση πακέτων είναι ότι για να πάρει η αντιπυρική ζώνη μια απόφαση φιλτραρίσματος, πρέπει να επιθεωρήσει κάθε πακέτο σε κάθε κατεύθυνση και σε όλες τις διεπαφές. Επίσης, για κάθε πακέτο που θα επιθεωρηθεί πρέπει να υπάρξουν κανόνες ελέγχου πρόσβασης. Αυτή η απαίτηση μπορεί να παρουσιάσει πρόβλημα όταν έρχεται η σειρά που πρέπει να καθοριστεί ένας κανόνας ελέγχου πρόσβασης για να εξεταστεί η επιστρεφόμενη κυκλοφορία από ένα επιτρεπόμενο αίτημα.

Συνδέσεις και κατάσταση: Για να επικοινωνήσουν δύο TCP/IP hosts πρέπει πρώτα να καθιερώσουν κάποια σύνδεση. Οι συνδέσεις εξυπηρετούν δύο

σκοπούς. Καταρχήν, μπορούν να χρησιμοποιήσουν τη σύνδεση για να προσδιοριστούν εκατέρωθεν. Ο προσδιορισμός εξασφαλίζει ότι τα συστήματα δεν παραδίδουν ακούσια τα στοιχεία στους hosts που δεν περιλαμβάνονται στη σύνδεση. Οι αντιπυρικές ζώνες μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες σύνδεσης για να καθορίσουν τις συνδέσεις που επιτρέπονται μεταξύ των hosts από την πολιτική ελέγχου πρόσβασης και έτσι να καθορίζουν εάν τα στοιχεία πρέπει να επιτραπούν ή να απορριφτούν.

Στη συνεχεία, οι συνδέσεις χρησιμοποιούνται για να καθορίσουν τον τρόπο με τον οποίο δύο hosts θα επικοινωνήσουν μεταξύ τους. Για το πρωτόκολλο ελέγχου μεταφοράς (TCP), αυτός ο τύπος σύνδεσης είναι γνωστός ως σύνοδος προσανατολισμένη προς τη σύνδεση (connection-oriented session). Για το πρωτόκολλο διαγραμμάτων δεδομένων χρηστών (UDP) και το πρωτόκολλο μηνυμάτων ελέγχου διαδικτύου (ICMP), αυτός ο τύπος σύνδεσης είναι γνωστός ως σύνοδος χωρίς σύνδεση (connectionless session).

Η προκαθορισμένη δομή μιας σύνδεσης μπορεί να χρησιμοποιηθεί για να καθορίσει την κατάσταση των επικοινωνιών μεταξύ δύο hosts. Για παράδειγμα όταν ο host A προσπαθεί να επικοινωνήσει με τον host B, ο A ξεκινά ένα αίτημα σύνδεσης. Έπειτα ο host B ανταποκρίνεται στο αίτημα σύνδεσης προσδιορίζοντας με αυτό τον τρόπο πώς οι δύο hosts θα γνωρίζουν τα δεδομένα που πρέπει να σταλούν καθώς και το πότε πρέπει να σταλούν. Το σχήμα 2-2 επεξηγεί λεπτομερώς αυτή τη διαδικασία:



Σχήμα 2-2 : Διαδικασία επικοινωνίας μεταξύ δυο host

1. Ο Host A αρχίζει μια σύνδεση προς το Host B.
2. Ο Host B ανταποκρίνεται στο αίτημα σύνδεσης από το Host A.
3. Ο Host A οριστικοποιεί τη σύνδεση με το Host B, επιτρέποντας τη μεταφορά των δεδομένων.
4. Ο Host A αρχίζει να μεταδίδει τα απαραίτητα δεδομένα στο Host B.
5. Ο Host B αποκρίνεται όπως απαιτείται, είτε με τα ζητούμενα δεδομένα, είτε για να αναγνωρίσει περιοδικά την παραλαβή των στοιχείων από το Host A.

Οι αντιπυρικές ζώνες μπορούν να παρακολουθήσουν τις πληροφορίες κατάστασης σύνδεσης για να καθορίσουν εάν θα επιτρέψουν ή θα αρνηθούν την κυκλοφορία. Παραδείγματος χάριν, όταν η αντιπυρική ζώνη βλέπει το πρώτο αίτημα σύνδεσης από το Host A (βήμα 1), γνωρίζει ότι το επόμενο στοιχείο που πρέπει να δει είναι η αναγνώριση του αιτήματος σύνδεσης από το Host B (βήμα 2). Αυτό γίνεται με τη χρήση ενός πίνακα κατάστασης (state table) που διατηρεί την κατάσταση όλων των συνομιλιών που διαπερνούν την αντιπυρική ζώνη. Με τον έλεγχο της κατάστασης συνομιλίας, η αντιπυρική ζώνη μπορεί να καθορίσει εάν τα δεδομένα που διακινούνται αναμένονται από το Host A. Εάν τα δεδομένα που περνούν δεν ταιριάζουν με την κατάσταση της συνομιλίας (όπως καθορίζεται από τον πίνακα κατάστασης), ή εάν το στοιχείο δεν είναι στον πίνακα, τα απορρίπτει. Αυτή η διαδικασία είναι γνωστή ως stateful inspection.

Stateful Packet Inspection (SPI): Η διαδικασία που οι αντιπυρικές ζώνες συνδυάζουν την stateful επιθεώρηση με την επιθεώρηση πακέτων, είναι γνωστή ως stateful επιθεώρηση πακέτων. Είναι στην ουσία η επιθεώρηση των πακέτων βασισμένη όχι μόνο στη δομή τους και τα δεδομένα που περιλαμβάνονται σε αυτά, αλλά βασισμένη και στην κατάσταση που είναι η συνομιλία μεταξύ των hosts. Κατά συνέπεια η επιθεώρηση επιτρέπει στις αντιπυρικές ζώνες να φιλτράρουν χρησιμοποιώντας όχι μόνο το περιεχόμενο του πακέτου, αλλά και τη σύνδεση ή τη κατάσταση στην οποία η θα είναι η σύνδεση στην συγκεκριμένη περίοδο. Παρέχει έτσι μια πιο ευέλικτη, συντηρήσιμη, και εξελικτική λύση φιλτραρίσματος.

Ένα άλλο όφελος της SPI σε σχέση με την απλή επιθεώρηση πακέτων που αναφέρθηκε προηγουμένως, είναι ότι όταν μια σύνδεση έχει προσδιοριστεί και επιτραπεί (εφόσον έχει επιθεωρηθεί αναλόγως), δεν είναι απαραίτητο να καθοριστεί ένας κανόνας για να επιτραπεί οι επιστρεφόμενη κίνηση επειδή η αντιπυρική ζώνη γνωρίζει από την κατάσταση τι πρέπει να είναι μια αποδεκτή απάντηση. Αυτή η διαδικασία γίνεται χωρίς να πρέπει να καθοριστεί ρητά κάποιος κανόνας για να επιτραπούν οι απαντήσεις και οι επόμενες επικοινωνίες. Οι περισσότερες αντιπυρικές ζώνες λειτουργούν σήμερα με αυτόν τον τρόπο.

2.3.2 Επικύρωση πρόσβασης

Το να θεωρηθεί η επιθεώρηση της IP διεύθυνσης προέλευσης και θύρας ως το ίδιο με την επικύρωση, ένα κοινό λάθος που γίνεται κατά την αξιολόγηση των αντιπυρικών ζωνών. Κάνοντας spoof μια IP διεύθυνση, κάποιο host θα μπορούσε να εμφανιστεί σαν να είναι εξ ολοκλήρου διαφορετικός host, παραμερίζοντας έτσι την επιθεώρηση ασφάλειας που θα ήταν βασισμένη στη διεύθυνση προέλευσης και θύρας. Για να αποβάλουν αυτό τον κίνδυνο, οι αντιπυρικές ζώνες πρέπει να παρέχουν επίσης και ένα μέσο επικύρωσης πρόσβασης. Το TCP/IP στηρίχτηκε στην προϋπόθεση των ανοικτών επικοινωνιών. Εάν δύο hosts γνωρίζουν εκατέρωθεν τις διευθύνσεις IP και συνδέονται ο ένας με τον άλλον, τότε μπορούν να επικοινωνήσουν. Αν και αυτό ήταν ένα ευγενές σχέδιο, στο σημερινό κόσμο μπορεί να μην θελήσουμε ο καθένας να είναι σε θέση να επικοινωνεί με τα συστήματα πίσω από την αντιπυρική ζώνη.

Οι αντιπυρικές ζώνες μπορούν να υποστηρίξουν την επικύρωση χρησιμοποιώντας διάφορους μηχανισμούς. Κατ' αρχάς, η αντιπυρική ζώνη μπορεί να απαιτήσει την εισαγωγή ενός ονόματος χρήστη και ενός κωδικού πρόσβασης (γνωστό ως εκτεταμένη επικύρωση ή xauth). Χρησιμοποιώντας την xauth, ο χρήστης που προσπαθεί να αρχίσει μια σύνδεση προτρέπεται για ένα όνομα χρήστη και έναν κωδικό πρόσβασης πριν η αντιπυρική ζώνη επιτρέψει σε μια σύνδεση να καθιερωθεί. Έτσι, αφού η σύνδεση έχει επικυρωθεί και

εξουσιοδοτηθεί από την πολιτική ασφάλειας, ο χρήστης δεν προτρέπεται πλέον για επικύρωση για την ιδία σύνδεση. Ένας άλλος μηχανισμός για την επικύρωση των συνδέσεων είναι μέσω της χρήσης πιστοποιητικών (certificates) και δημόσιων κλειδιών (public keys). Το όφελος των πιστοποιητικών σε σχέση με τη xauth είναι η διαδικασία επικύρωσης, η οποία μπορεί να γίνει χωρίς την επέμβαση χρηστών. Προϋπόθεση για το τελευταίο είναι οι hosts να έχουν διαμορφωθεί με τα αντίστοιχα πιστοποιητικά και μαζί με την αντιπυρική ζώνη να χρησιμοποιούν μια κατάλληλα διαμορφωμένη υποδομή δημόσια κλειδιού (public key infrastructure). Ένα όφελος αυτής της προσέγγισης είναι ότι μπορεί να κλιμακωθεί πολύ καλύτερα για μεγάλες εφαρμογές.

Επιπλέον, η επικύρωση μπορεί να αντιμετωπιστεί μέσω της χρήσης των προ-μοιραζόμενων κλειδιών (pre-shared keys PSK). Τα PSK είναι λιγότερο σύνθετα για να εφαρμόσουν από τα πιστοποιητικά, επιτρέποντας συγχρόνως στη διαδικασία επικύρωσης να γίνει χωρίς την επέμβαση των χρηστών. Με τα PSK, στον host παρέχεται ένα προκαθορισμένο κλειδί που χρησιμοποιείται για τη διαδικασία επικύρωσης. Ένα μειονέκτημα αυτού του συστήματος είναι ότι το PSK αλλάζει σπάνια και πολλές οργανώσεις χρησιμοποιούν το ίδιο κλειδί σε μεγάλο αριθμό host, υπονομεύοντας κατά συνέπεια την ασφάλεια της διαδικασίας επικύρωσης. Με την εφαρμογή της επικύρωσης, η αντιπυρική ζώνη έχει μια πρόσθετη μέθοδο για να καθορίσει εάν μια σύνδεση πρέπει να επιτραπεί. Ακόμα και όταν θα επιτρεπόταν το πακέτο βάσει στην επιθεώρηση της κατάσταση σύνδεσης, εάν ο host δεν μπορέσει να επικυρωθεί επιτυχώς με την αντιπυρική ζώνη, τότε το πακέτο θα απορριφθεί.

2.3.3 Λειτουργία μεσολαβητή

Όταν οι άνθρωποι ανησυχούν ότι μια άμεση συνάντηση θα ήταν πολύ επικίνδυνη, χρησιμοποιούν συνήθως τους ενδιάμεσους/μεσολαβητές για να ενεργήσουν εξ ονόματός τους και να τους προστατεύουν από τον κίνδυνο της άμεσης αλληλεπίδρασης. Στο ίδιο πνεύμα, μια αντιπυρική ζώνη μπορεί να διαμορφωθεί για να ενεργήσει ως μεσολαβητής στη διαδικασία επικοινωνίας

μεταξύ δύο hosts. Αυτή η διαδικασία μεσολάβησης αναφέρεται συνήθως ως λειτουργία proxy. Ένα proxy λειτουργεί αποτελεσματικά μιμούμενος τον host που προσπαθεί να προστατεύσει. Όλες οι επικοινωνίες που προορίζονται για τον προστατευμένο host γίνονται μέσω του proxy, το οποίο εμφανίζεται στον απομακρυσμένο host σαν να είναι το προστατευμένο host. Έτσι, ο μακρινός host δεν έχει κανέναν τρόπο να καταλάβει ότι δεν μιλά άμεσα στον προστατευμένο πόρο.

Σε πολλές περιπτώσεις, η λειτουργία του proxy συμπληρώνεται με τη χρησιμοποίηση μιας αντιπυρικής ζώνης που είναι σε θέση να εξασφαλίσει εάν ένα στοιχείο είναι νόμιμο και όχι κακόβουλο (nonmalicious). Όταν λειτουργεί με αυτόν τον τρόπο, η αντιπυρική ζώνη είναι γνωστή ως application proxy. Η λειτουργία αυτής της μορφής επιτρέπει στην αντιπυρική ζώνη να επιθεωρήσει από μόνη της τα πραγματικά δεδομένα εφαρμογής (application data) πριν παρουσιάσει τα δεδομένα αυτά στον προστατευμένο host.

2.3.4 Προστασία πόρων

Η σημαντικότερη ευθύνη μιας αντιπυρικής ζώνης είναι να προστατευθούν οι πόροι ενός συστήματος η οργανισμού από τις διαφορές απειλές. Αυτή η προστασία επιτυγχάνεται μέσω της χρήσης κανόνων ελέγχου πρόσβασης, της stateful επιθεώρησης πακέτων, της πληρεξούσιας εφαρμογής (application proxies), ή συνδυασμού τους. Οι αντιπυρικές ζώνες δεν είναι μια αλάνθαστη μέθοδος και δεν πρέπει κάποιος να στηριχθεί αποκλειστικά στην αντιπυρική ζώνη για να προστατεύσει ένα δίκτυο. Εάν κάποιο host, που του λείπουν οι κατάλληλες επιδιορθώσεις προγραμμάτων (unpatched host) συνδέεται με το διαδίκτυο, τότε μια αντιπυρική ζώνη μπορεί να μην είναι σε θέση να τον αποτρέψει από την έκθεση και εκμετάλλευση (exploited), ειδικά εάν ο host χρησιμοποιεί κυκλοφορία για την οποία η αντιπυρική ζώνη έχει διαμορφωθεί να επιτρέψει.

Για παράδειγμα, εάν μια αντιπυρική ζώνη πακέτο-επιθεώρησης (packet-inspecting firewall) επιτρέπει την κυκλοφορία HTTP προς ένα unpatched web διακομιστή, κάποιος κακόβουλος χρήστης θα μπορούσε να κάνει χρήση μιας επίθεσης που βασίζεται στο HTTP για να «χτυπήσει» τον διακομιστή αφού ο τελευταίος δεν είναι επιδιορθωμένος ενάντια σε αυτή τη νέα απειλή. Ο διακομιστής σε αυτήν την περίπτωση καθιστά την αντιπυρική ζώνη άχρηστη ως συσκευή προστασίας. Για αυτόν τον λόγο, εκτός από την προστασία από μια αντιπυρική ζώνη, οι προστατευμένοι πόροι πρέπει πάντα να κρατηθούν επιδιορθωμένοι και ενημερωμένοι στης αλλαγές.

2.3.5 Καταγραφή και αναφορά συμβάντων

Ανεξάρτητα από το τι κάνουμε για να προστατεύουμε τους πόρους με μια αντιπυρική ζώνη, η πραγματικότητα είναι δεν μπορούμε να σταματήσουμε κάθε κακόβουλη πράξη ή όλα τα κακόβουλα στοιχεία. Είτε από λάθος ρυθμίσεις (misconfigurations) είτε από καινούριες απειλές που η αντιπυρική ζώνη δεν μπορεί ακόμα να μας προστατεύσει, πρέπει να είμαστε προετοιμασμένοι να εξετάσουμε και αντιμετωπίσουμε ένα γεγονός ασφάλειας που η αντιπυρική ζώνη δεν ήταν ικανή να αποτρέψει. Κατά συνέπεια, όλες οι αντιπυρικές ζώνες πρέπει να έχουν μια μέθοδο καταγραφής για όλες τις επικοινωνίες που εμφανίζονται, ώστε να επιτρέψει στο διαχειριστή (administrator) να εξετάσει τα καταγραμμένα στοιχεία, σε μία προσπάθεια να εξακριβωθεί τι έλαβε χώρα.

Η καταγραφή των γεγονότων (events) μπορεί να γίνει με διάφορους τρόπους, αλλά οι περισσότερες αντιπυρικές ζώνες χρησιμοποιούν δύο μεθόδους, είτε syslog είτε κάποιο ιδιόκτητο σχήμα αναγραφών. Εκτός από τα οφέλη της ανάλυσης των γεγονότων, τα στοιχεία μπορούν επίσης να χρησιμοποιηθούν και για την ανίχνευση λαθών μιας αντιπυρικής ζώνης (troubleshooting) ώστε να βοηθήσουν στην ανακάλυψη της αιτίας του προβλήματος που εμφανίστηκε. Μερικά γεγονότα είναι αρκετά σημαντικά και η πολιτική της απλής καταγραφής δεν είναι αρκετή. Εκτός από την καταγραφή του γεγονότος, η αντιπυρική ζώνη πρέπει επίσης να έχει έναν μηχανισμό συναγερμού όταν παραβιαστεί μια

πολιτική. Οι αντιπυρικές ζώνες πρέπει να υποστηρίξουν διάφορους τύπους συναγερμών:

- Ειδοποίηση στη κονσόλα: Το μειονέκτημα αυτής της μεθόδου είναι ότι απαιτεί να ελέγχει κάποιος ενεργά την κονσόλα για να καταλάβει ότι έχει παραχθεί συναγερμός.
- Ειδοποίηση SNMP: Το SNMP μπορεί να χρησιμοποιηθεί για να παραγάγει τις παγίδες (traps) που στέλνονται σε ένα σύστημα διαχείρισης δικτύων (NMS) που ελέγχει την αντιπυρική ζώνη.
- Ειδοποίηση σελιδοποίησης: Για κάθε νέο γεγονός, η αντιπυρική ζώνη μπορεί να διαμορφωθεί ώστε να στείλει μια σελίδα στο διαχειριστή.
- Ειδοποίηση ηλεκτρονικού ταχυδρομείου: Παρόμοια με τη σελιδοποίηση αλλά σε αυτή τη περίπτωση η αντιπυρική ζώνη στέλνει ένα e-mail.

Από την ύπαρξη μιας μεθόδου καταγραφής και αναφοράς γεγονότων, η αντιπυρική ζώνη μπορεί να παρέχει ένα λεπτομερές επίπεδο διορατικότητας ως προς αυτό που εμφανίζεται εκείνη τη στιγμή, ή προηγουμένως σε περίπτωση που πρέπει να εκτελεσθεί μια δικανική ανάλυση (forensic analysis).

2.4 Ποιες είναι οι απειλές;

Το να γνωρίζουμε μόνο το τι κάνει μια αντιπυρική ζώνη ή το πώς λειτουργεί δεν είναι αρκετό. Πρέπει να κατανοήσει κάνεις και τις απειλές που υπάρχουν, ώστε να εξασφαλιστεί ότι μπορεί να προστατεύει αποτελεσματικά το περιβάλλον του από τις απειλές. Οι απειλές που οι περισσότεροι οργανώσιμοι πρέπει να αντιμετωπίσουν περιλαμβάνουν τα εξής:

1. Στοχευόμενες η τυχαίες επιθέσεις
2. Κακόβουλα προγράμματα
3. Άρνηση υπηρεσίας
4. Social Engineering
5. Νέες απειλές

2.4.1 Στοχευόμενες η τυχαίες επιθέσεις

Επιφανειακά, η διαφορά μεταξύ στοχευόμενης και τυχαίας επίθεσης μπορεί να φανεί αρκετά ασήμαντη. Γενικά, μια επίθεση είναι πάντα μια επίθεση, ανεξάρτητα από την πηγή. Ωστόσο, είναι σημαντικό να καθοριστεί η διαφορά επειδή μπορεί να επηρεάσει το τελικό επίπεδο απάντησης που χρειάζεται για να διευθετηθεί μια επίθεση. Οι τυχαίες επιθέσεις (untargeted) είναι αυτές που δεν παρακινούνται άμεσα από τους πόρους που επιτίθενται. Με άλλα λόγια, ο επιτιθέμενος δεν παρακινείται απαραιτήτως για να επιτεθεί στους πόρους, αλλά προσπαθεί πιθανώς να αποκτήσει πρόσβαση σε οποιοδήποτε κεντρικό υπολογιστή που θα είναι ευαίσθητος. Κατά συνέπεια, αυτού του είδους επιθέσεις συνήθως δεν κρύβουν πίσω τους μεγάλη προσπάθεια και κίνητρο και μπορεί να είναι ευκολότερη η υπεράσπιση σε σχέση με μια στοχευόμενη επίθεση. Στις περισσότερες περιπτώσεις για μια αποτελεσματική υπεράσπιση ενάντια στην επίθεση αρκεί μόνο να απορριφθεί η κακόβουλη κυκλοφορία και να αναγκαστεί ο επιτιθέμενος να κινηθεί προς ευκολότερους λόγους κυνηγιού.

Οι στοχευόμενες επιθέσεις παρουσιάζουν μια πρόσθετη πλοκή στην επίθεση. Ο επιτιθέμενος ενδιαφέρεται για τους πόρους και τα δεδομένα και καταβάλει συνειδητή προσπάθεια στον στόχο να αποκτήσει πρόσβαση σε εκείνους τους πόρους. Αυτό κάνει μια στοχευόμενη επίθεση περισσότερο ανησυχητική επειδή γενικά σημαίνει ότι ο επιτιθέμενος πρόκειται να συνεχίσει να προσπαθεί για να αποκτήσει πρόσβαση σε εκείνους τους πόρους, παρά τις προσπάθειές μας για προστασία.

2.4.2 Κακόβουλα προγράμματα (malicious codes)

Είναι τα προγράμματα εκείνα που εκτελούν καταστροφικές ενέργειες σε υπολογιστικά συστήματα. Παρακάτω γίνεται μια αναφορά στους βασικούς τύπους κακόβουλων προγραμμάτων.

Ιοί (viruses): τα μέρη κώδικα που είναι προσαρτημένα σε ένα κανονικό πρόγραμμα και αντιγράφονται από μόνα τους. Μπορούν να δρουν καταστροφικά ή όχι. Είδη ιών:

- Ιοί εκκίνησης (bootstrap viruses): κώδικας που εισάγεται στην διαδικασία εκκίνησης ενός υπολογιστή.
- Παρασιτικοί ιοί (parasitic viruses): μέρη κώδικα που προσαρτώνται σε εκτελέσιμα προγράμματα.
- Συνοδευτικοί ιοί (companion viruses): εναλλακτικά εκτελέσιμα προγράμματα που εισάγονται στη διαδρομή αναζήτησης κανονικών προγραμμάτων.
- Ιοί μακροεντολών (macro viruses): τμήματα κώδικα που εισάγονται σε αρχεία δεδομένων τα οποία επεξεργάζεται μια εφαρμογή που υποστηρίζει μακροεντολές.

Δούρειοι ίπποι (trojan horses): προγράμματα που ενώ επικαλούνται ότι εκτελούν κάποια εργασία, στην πραγματικότητα εκτελούν και/ή άλλη εργασία.
Σκουλήκια (warms): προγράμματα που εξαπλώνονται μέσω των δικτυακών επικοινωνιών, αντιγράφοντας τα ίδια ανεξέλεγκτα. Προκαλούν καταστροφή αρχείων, υποκλοπή πληροφοριών και αποδιοργάνωση λειτουργιών συστήματος ώστε να προκαλείται άρνηση εξυπηρέτησης.

Λογικές βόμβες (logic bombs): προγράμματα που εκτελούνται όταν ικανοποιηθεί μια λογική συνθήκη.
Χρονικές βόμβες (time bombs): προγράμματα που εκτελούνται όταν έρθει κάποια κατάλληλη χρονική στιγμή.
Πίσω πόρτες (backdoors): κρυμμένες λειτουργίες προγραμμάτων με τις οποίες παρέχεται η προσπέλαση «ευαίσθητων» πληροφοριών.

Οι ιοί τα σκουλήκια, και οι δούρειοι ίπποι μπορεί να είναι δύσκολο να αντιμετωπιστούν μόνο με τη χρησιμοποίηση αντιπυρικών ζωνών και να απαιτήσουν, είτε την χρήση λογισμικού ιό-ανίχνευσης (virus-scanning software) στην ίδια την αντιπυρική ζώνη, είτε τη χρήση προϊόντων τρίτων (third-party)

που θα επεμβαίνουν από κοινού με μια αντιπυρική ζώνη. Αντίθετα από τις περισσότερες απειλές, για να επιτραπεί στο περιεχόμενο των malicious content και malware να εκτελεσθεί απαιτείτε από το χρήστη στο προστατευμένο δίκτυο να τα εκτελέσει, εσκεμμένα ή ακούσια. Κατά συνέπεια, η προστασία συχνά απαιτεί από την αντιπυρική ζώνη να είναι σε θέση να επιτηρήσει και να ελέγξει την κυκλοφορία που μπορεί να προέλθει από ένα προστατευμένο δίκτυο ή host. Συνήθως αυτό πραγματοποιείται μέσω της χρήσης των φίλτρων εξόδου (egress filters) στην ίδια την αντιπυρική ζώνη και λογισμικό content-filtering που χρησιμοποιείται από κοινού με την αντιπυρική ζώνη.

2.4.3 Άρνηση της υπηρεσίας (DoS)

Η επίθεση DoS αποτελεί μια απειλή που αποτρέπει τη νόμιμη κυκλοφορία από το να είσαι σε θέση να προσεγγιστεί το προστατευμένο πόρο. Μια διαδομένη επίθεση DoS μπορεί να αναγκάσει τις υπηρεσίες ενός διακομιστή να μην λειτουργούν, κάνοντας κατά συνέπεια την παρεχόμενη υπηρεσία απρόσιτη. Αυτή η επίθεση γίνεται συνήθως με την εκμετάλλευση των buffer overflows στο λογισμικό και πρωτόκολλα ή με την αποστολή αυξανόμενων δεδομένων στον host μέχρι που να μην μπορεί να αποκριθεί.

Μια δημοφιλές παραλλαγή του DoS και πιο δύσκολη στην αντιμετώπιση είναι το διανεμημένο DoS (DDoS). Ο τελικός σκοπός μπορεί να είναι και σε αυτή την περίπτωση ο ίδιος, αλλά η μέθοδος επίθεσης διαφέρει. Οι DDoS επιθέσεις χρησιμοποιούν χιλιάδες hosts για να επιτεθούν σε έναν στόχο, αυξάνοντας κατά συνέπεια εκθετικά το ποσό κυκλοφορίας. Ο σκοπός του DDoS είναι να υπερφορτωθεί ο στόχος με τόσα πολλά ψευδή αιτήματα ώστε να μην μπορεί να ανταποκριθεί στα νόμιμα αιτήματα.

Συνεπώς, η διαφορά μεταξύ ενός DoS και ενός DDoS είναι γενικά ο αριθμός των hosts που συμμετέχουν στην επίθεση και το γεγονός ότι οι επιτιθέμενοι επεκτείνονται σε αυτά τα συστήματα σε αντίθεση με τις επιθέσεις που προέρχονται από έναν ενιαίο επιτιθέμενο. Στην πραγματικότητα, πολλές

επιθέσεις DDoS δεν είναι τίποτα περισσότερο από ένα DoS που εκτελείται σε μια πολύ μεγαλύτερη κλίμακα. Ο πιο αποτελεσματικός τρόπος προστασίας από επίθεσης DDoS (π.χ. τύπου SYN flood) είναι η αύξηση του εύρος ζώνης και να το φιλτράρισμα της κακόβουλης κυκλοφορίας πριν διαπεράσει στα τμήματα δικτύων. Οι πιο διαδεδομένες μορφές DoS, μπορούν να αντιμετωπιστούν με την εφαρμογή των κατάλληλων κανόνων στην αντιπυρική ζώνη.

2.4.4 Social Engineering

Ως «Social Engineering» στον τομέα της ασφάλειας πληροφοριών και πληροφοριακών ή τηλεπικοινωνιακών συστημάτων έχει επικρατήσει να αποκαλείται η πρακτική της υφαρπαγής εμπιστευτικών πληροφοριών κατόπιν εξαπάτησης των υποκειμένων των εμπιστευτικών πληροφοριών. Ο όρος «Social Engineering» χρησιμοποιήθηκε από crackers που εξαπατούσαν τα θύματά τους μέσω τηλεφωνικών συνδιαλέξεων. Σήμερα, χρησιμοποιείται ο ίδιος όρος για την εξαπάτηση των καταναλωτών μέσω Διαδικτύου.

Ο social engineer χρησιμοποιώντας συνήθως το τηλέφωνο ή το διαδίκτυο, εξαπατά τους καταναλωτές οδηγώντας τους με απατηλές μεθόδους στην αποκάλυψη εμπιστευτικών πληροφοριών, συμπεριλαμβανομένων προσωπικών και ευαίσθητων δεδομένων, ή κατευθύνοντάς τους παραπειστικά για να ενεργήσουν πράξεις αντίθετες σε πολιτικές ασφαλείας συστημάτων, με σκοπό τη χρήση των πληροφοριακών δεδομένων των θυμάτων για την επίτευξη περιουσιακού οφέλους στον ίδιο ή σε τρίτον. Λόγω της φύσης μιας social-engineering επίθεσης, οι αντιπυρικές ζώνες δεν μπορούν να κάνουν τίποτα για να αποτρέψουν την επίθεση. Η καλύτερη υπεράσπιση είναι η εκπαίδευση των χρηστών και προσωπικό ώστε γνωρίζουν ποιες είναι οι αποδεκτές πληροφορίες που μπορεί να κοινοποιηθούν.

2.4.5 Νέες απειλές

Ένας τρέχων θέμα είναι η απειλή του γεγονότος μηδενικής-ημέρας (zero-day). Το γεγονός μηδενικής-ημέρας είναι μια ευπάθεια ασφάλειας που αξιοποιείται την ίδια ημέρα που αύτη ανακαλύπτεται, δηλαδή προτού μπορέσουν οι προμηθευτές (vendors) του συστήματος να αποκριθούν με τη κατάλληλη λύση (patch). Ο χρόνος από την ευπάθεια στην εκμετάλλευση αποτελεί πρόβλημα επειδή οι περισσότερες τεχνολογίες σήμερα απαντούν με μια μάλλον αντιδραστική μορφή στις επιθέσεις. Όταν οι νέες ευπάθειες ανακαλύπτονται και δημοσιεύονται, οι προμηθευτές πρέπει συχνά να υπολογίσουν τη λύση και να προσπαθήσουν να την παραδώσουν προτού γίνει η επίθεση. Κατά τη διάρκεια αυτής της περιόδου τα συστήματα είναι απολύτως τρωτά και ευαίσθητα σε επιθέσεις και εκμετάλλευση. Ο μόνος αποτελεσματικός τρόπος να εξεταστούν αυτές οι επίθεσης είναι να εξασφαλιστεί η υπάρξει μιας επιθετικής patch λύσης (aggressive patch) και ότι οι ανανεωμένοι κανόνες ελέγχου θα εφαρμοστούν έγκαιρα, μειώνοντας κατά συνέπεια την περίοδο ευπάθειας.

2.5 Είδη και κίνητρα εισβολέων

Υπάρχουν δύο ειδών εισβολείς. Οι παθητικοί εισβολείς, οι οποίοι απλώς θέλουν να διαβάσουν αρχεία για τα οποία δεν έχουν αυτού του είδους την εξουσιοδότηση. Οι ενεργοί εισβολείς είναι πιο κακόβουλοι και θέλουν να κάνουν μη εξουσιοδοτημένες αλλαγές σε δεδομένα. Κατά το σχεδιασμό της ασφάλειας ενός συστήματος, πρέπει να γνωρίζουμε το είδος και τα κίνητρα του εισβολέα από τον οποίο θέλουμε να προστατευθούμε. Ορισμένες κοινές κατηγορίες είναι:

- Περίεργοι χρήστες χωρίς τεχνικές γνώσεις. Πολλοί χρήστες, εξαιτίας της ανθρώπινης φύσης, θα θελήσουν να διαβάσουν το ηλεκτρονικό ταχυδρομείο και τα αρχεία άλλων ανθρώπων, αν δεν υπάρχει κανένας φραγμός για αυτό.

- Προσπάθεια προσπέλασης από εσωτερικούς εισβολείς. Οι φοιτητές, οι προγραμματιστές συστημάτων, οι χειριστές και το λοιπό τεχνικό προσωπικό, συχνά θεωρούν ως προσωπική πρόκληση την παράκαμψη της ασφάλειας του τοπικού υπολογιστικού συστήματος. Συχνά έχουν υψηλά προσόντα και είναι αποφασισμένοι να αφιερώσουν ένα σημαντικό μέρος του χρόνου τους στην προσπάθεια αυτή.

- Ηθελημένες προσπάθειες για οικονομικά οφέλη. Παράδειγμα της συγκεκριμένης μορφής είναι η υπάρξει μηχανικών που εργάζονται σε τράπεζες και προσπαθούν να μπουν σε κάποιο σύστημα με σκοπό να κλέψουν από αυτή.

- Εμπορική ή στρατιωτική κατασκοπία. Η κατασκοπία συνίσταται σε μια σοβαρή και με οργανωμένη προσπάθεια ενός ανταγωνιστή ή μιας ξένης χώρας με στόχο να κλαπούν σημαντικοί πώροι.

2.6 Πολιτικές ασφάλειας

Οι αντιπυρικές ζώνες δεν είναι τίποτα περισσότερο από τα σημεία πολιτικής επιβολής ελέγχου πρόσβασης. Συνεπώς, μια αντιπυρική ζώνη είναι τόσο αποτελεσματική όσο η πολιτική ασφάλειας (security policy) που θα υπαγορεύει το πώς θα χρησιμοποιηθεί η αντιπυρική ζώνη. Το πρώτο βήμα σε μια πετυχημένη πολιτική ασφάλειας είναι η ανάλυση κινδύνου (risk analysis), η οποία και θα καθορίσει τις απειλές για το προστατευμένο σύστημα. Μετά από αυτό, μπορεί να αναπτυχθεί η στρατηγική και η πολιτική για την προστασία του συστήματος από τις αντιπυρικές ζώνες για τις αντίστοιχες απειλές.

Ένα βασικό στοιχειό που θα πρέπει να γίνει αντιληπτό κατά την ανάπτυξη της στρατηγικής είναι ότι μπορεί να μην είμαστε σε θέση να προστατευτούμε ή να αποτρέψετε όλες τις επιθέσεις. Οι λόγοι ξεκινούν από τους τεχνολογικούς περιορισμούς και φτάνουν στους πρακτικούς και οικονομικούς περιορισμούς. Κατά συνέπεια, το θέμα θα πρέπει να εξεταστεί από την προοπτική της

επιδίωξης να ελαχιστοποιηθεί ο κίνδυνος που συνδέεται με την απειλή. Σε μερικές περιπτώσεις, αυτό σημαίνει ότι ο κίνδυνος μπορεί να μειωθεί στο μηδέν (πχ, εάν χρησιμοποιηθεί μια αντιπυρική ζώνη για να αποτρέψει όλη την πρόσβαση σε ένα σύστημα). Σε άλλες περιπτώσεις, μπορούμε μόνο να μειώσουμε τον κίνδυνο σε ένα επίπεδο που θα είναι αποδεκτό για το δίκτυο.

2.7 Αντιπυρικές ζώνες και εμπιστοσύνη

Με την λήψη απόφασης που επιτρέπει την κυκλοφορία μέσω της αντιπυρικής ζώνης, ο διαχειριστής έχει λάβει και την απόφαση (σκόπιμη ή όχι) να εμπιστευθεί την κυκλοφορία αυτή. Η παρούσα απόφαση είναι μέρος του καθορισμού ενός αποδεκτού επιπέδου κινδύνου. Μια αντιπυρική ζώνη δεν υπάρχει για να σταματήσει όλη την κυκλοφορία, αλλά για να επιτρέψει κάποια κυκλοφορία σταματώντας κάποια άλλη. Αυτό δεν σημαίνει ότι με μια απόφαση που επιτρέπει κάποια κυκλοφορία αφαιρούμε την ασφάλεια που μπορεί να παρέχει μια αντιπυρική ζώνη.

Στη συνεχή αναζήτηση της ελαχιστοποίησης του κινδύνου, η αντιπυρική ζώνη μπορεί να διαμορφωθεί ώστε να επικυρώνει τις συνδέσεις που έχουν πρόσβαση στον εμπιστευόμενο σύστημα η πώρο. Να εξασφαλιστεί έτσι ότι προτού χορηγηθεί κάποια πρόσβαση στον προστατευμένο πόρο, το σύστημα που κάνει την αίτηση πρέπει να επικυρωθεί ως νόμιμος και έγκυρος χρήστης του τελικού συστήματος . Μια άλλη επιλογή είναι να χρησιμοποιηθεί η αντιπυρική ζώνη ως proxy, λειτουργώντας ως ένας μεσάζων για την παροχή της πρόσβασης στον προστατευμένο σύστημα. Το σημείο που θα πρέπει να αποτελέσει και κανόνα για τις αντιπυρικές ζώνες και την εμπιστοσύνη είναι ότι όσο και να εμπιστευόμαστε την πρόσβαση που χορηγείται, αύτη θα πρέπει να περάσει από την αντιπυρική ζώνη πριν αποκτήσει έλεγχο στον προστατευμένο σύστημα.

2.8 Καθορισμός αναγκαιότητας μιας αντιπυρικής ζώνης

Το να ειπωθεί ότι μια αντιπυρική ζώνη χρειάζεται μόνο όταν υπάρχει σύνδεση με το διαδίκτυο θα ήταν ανακριβές. Οι αντιπυρικές ζώνες δεν πρέπει να συνδεθούν αποκλειστικά με το κομμάτι της παροχής πρόσβασης και την προστασία των συστημάτων που συσχετίζονται με το διαδίκτυο. Αντίθετα, πρέπει να εξεταστεί η χρήση μιας αντιπυρικής ζώνης κάθε φορά που πρέπει να προστατευθεί ένας σύστημα, ανεξάρτητα από το που βρίσκεται, ή από πού θα προέρχεται η αίτηση της κυκλοφορίας. Σε πολλές περιπτώσεις οι αντιπυρικές ζώνες μπορούν και πρέπει να χρησιμοποιηθούν για να ελέγξουν την πρόσβαση στους σημαντικούς κεντρικούς υπολογιστές ή τα διαφορετικά υποδίκτυα μέσα σε ένα εταιρικό δίκτυο (corporate network).

Για να καθορίσουμε που μπορεί να εφαρμοστεί μια αντιπυρική ζώνη, θα πρέπει πρώτα να οριστεί το κόστος των στοιχείων που προσπαθούμε να προστατεύσουμε. Αυτό το κόστος περιλαμβάνει διάφορες μεταβλητές. Μια μεταβλητή είναι το κόστος της αποκατάστασης και επιδιόρθωσης των δεδομένων. Μια πρόσθετη μεταβλητή είναι το κόστος της χαμένων εργασιών και του χρόνου διακοπής ως αποτέλεσμα των στοιχείων που είναι απρόσιτα στους υπαλλήλους. Ακόμα μια μεταβλητή είναι το κόστος στο χαμένο εισόδημα ή το εισόδημα που θα προκύψει ως αποτέλεσμα της απώλειας δεδομένων.

Το κόστος του «starting over» αποτελεί μια μεταβλητή ιδιαίτερα σημαντική για τις μικρότερες επιχειρήσεις. Η πλειοψηφία τους που θα πρέπει να αντιμετωπίσει, ως αποτέλεσμα ενός γεγονότος ασφάλειας, την διαδικασία διακοπής (downtime) για μια εβδομάδα είναι σπάνια ικανή να επανέλθει από τη διακοπή λειτουργίας και ακολούθως θα παρεκτραπεί από τους οικονομικούς στόχους. Το κόστος του νομικού αντίκτυπου ως αποτέλεσμα της απώλειας ή της έκθεσης σε τρίτους στοιχείων, είναι ένα άλλο πραγματικό κόστος που πρέπει επίσης να εξεταστεί. Η απλή πραγματικότητα είναι ότι ζούμε σε μια φιλόδικη κοινωνία, και εάν μια επιχείρηση είναι αμελής από το να προστατεύσει επαρκώς τα ευαίσθητα δεδομένα της, ειδικά εάν αυτά είναι στοιχεία καταναλωτών, τότε μπορεί να βρεθεί αντιμέτωπη με την οικονομική αποζημίωση των τελευταίων.

ΚΕΦΑΛΑΙΟ 3

Κατηγοριοποίηση αντιπυρικών ζωνών

3.1 Εισαγωγή

Το κεφάλαιο αυτό καλύπτει την κατηγοριοποίηση των αντιπυρικών ζωνών. Οι αντιπυρικές ζώνες μπορούν να κατηγοριοποιηθούν σε διάφορες κατηγορίες, από το μέγεθος του δικτύου που θα λειτουργήσουν έως τον τρόπο που παρέχουν προστασία. Εξετάζει τη βασική ταξινόμηση των αντιπυρικών ζωνών σε αντιπυρικές ζώνες για προσωπικούς υπολογιστές, μικρούς οργανισμούς (small office/home office - SOHO) και μεγάλους οργανισμούς. Επιπλέον, αναλύει τους τρόπους που οι αντιπυρικές ζώνες υπερασπίζονται τα δίκτυα, όπως τα απλά φίλτρα πακέτων, stateful φίλτρα πακέτων και πληρεξούσια εφαρμογής (application proxies). Παρέχει επίσης και μια επισκόπηση των διάφορων προϊόντων αντιπυρικών ζωνών.

3.2 Ταξινόμηση αντιπυρικών ζωνών

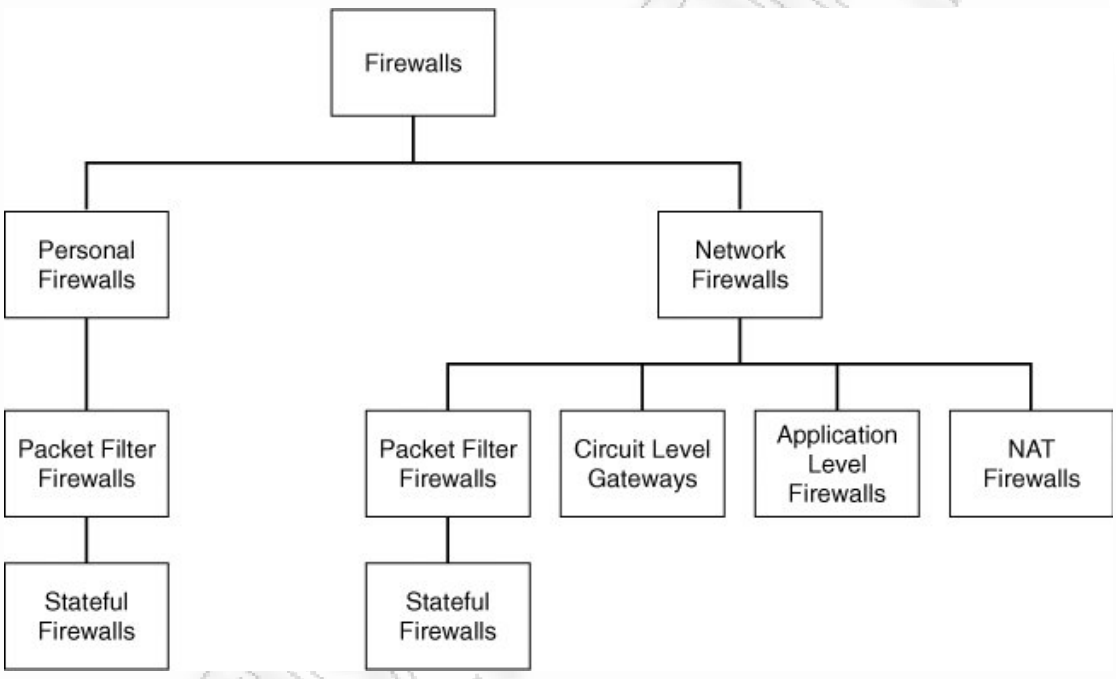
Οι αντιπυρικές ζώνες μπορούν να ταξινομηθούν κάτω από δύο γενικούς τύπους:

1. Προσωπικές αντιπυρικές ζώνες (Personal firewalls)
2. Αντιπυρικές ζώνες δικτύων (Network firewalls)

Η αρχική διαφορά μεταξύ αυτών των δύο τύπων αντιπυρικών ζωνών είναι στον αριθμό των υπολογιστών που προστατεύει η αντιπυρική ζώνη. Στις αντιπυρικές ζώνες δικτύων, συμπεριλαμβανομένων οι παρακάτω τύποι:

- Αντιπυρικές ζώνες φιλτραρίσματος πακέτων (Packet-filtering firewalls)
- Πύλες επιπέδου συνόδου (Circuit-level gateways)
- Πύλες επιπέδου εφαρμογής (Application-level gateways)

Η παραπάνω ταξινόμηση περιγράφει τις γενικές κατηγορίες αντιπυρικών ζωνών. Πολλές αντιπυρικές ζώνες δικτύων χρησιμοποιούν υβριδικές τεχνικές και έχουν χαρακτηριστικά που τις τοποθετούν σε περισσότερες από μια ταξινομήσεις. Το σχήμα 3-1 παρουσιάζει μια ανάλυση των διάφορων τύπων αντιπυρικών ζωνών, που υπάρχουν σήμερα διαθέσιμα, με κριτήριο τους δύο αρχικούς τύπους: προσωπικές αντιπυρικές ζώνες και αντιπυρικές ζώνες δικτύων.



Σχήμα 3-1 : Ταξινόμηση αντιπυρικών ζωνών

3.2.1 Προσωπικές αντιπυρικές ζώνες

Οι προσωπικές αντιπυρικές ζώνες σχεδιάζονται για να προστατεύσουν ένα σύστημα από μη εξουσιοδοτημένη πρόσβαση. Οι σύγχρονες προσωπικές αντιπυρικές ζώνες για να προστατεύσουν μια συσκευή ενσωματώνουν πρόσθετες ικανότητες όπως ο έλεγχος λογισμικού για ιούς και σε μερικές περιπτώσεις ανάλυση συμπεριφοράς (behavior analysis) και ανίχνευση παρείσφρησης (intrusion detection). Μερικές από τις δημοφιλέστερες εμπορικές προσωπικές αντιπυρικές ζώνες είναι τα BlackICE και Cisco Security Agent. Για την κατηγορία SOHO τα δημοφιλέστερα προϊόντα είναι το PC-Cillin της Trend

Micro, ZoneAlarm, Symantec personal firewall και Internet Connection Firewall της Microsoft.

Σε μια μεγάλη επιχείρηση η οργανισμό τα ζητήματα είναι πιο σύνθετα. Ίσως η μεγαλύτερη ανησυχία για τους επιχειρηματικούς χρήστες, όσον αφορά τις προσωπικές αντιπυρικές ζώνες, είναι η δυνατότητα να παρασχεθεί ένας συγκεντρωτικός μηχανισμός πολίτικης ελέγχου. Σε ένα επιχειρηματικό περιβάλλον υπάρχει η ανάγκη να συγκεντρωθεί η πολιτική έλεγχου για τη χρήση των προσωπικών αντιπυρικών ζωνών ώστε να ελαχιστοποιήσει το φορτίο διαχείρισης. Δεδομένου ότι ο αριθμός των αντιπυρικών ζωνών που υπάρχουν σε μια οργάνωση αυξάνεται, ο διαχειριστής δικτύων πρέπει να ενδιαφερθεί για την κατάλληλη διαμόρφωση και τον έλεγχο της κάθε αντιπυρικής ζώνης. Επομένως, η δυνατότητα να αντιμετωπιστούν χωρίς υπερβολικό εργασιακό φόρτο είναι εξαιρετικά σημαντική.

3.2.2 Αντιπυρικές ζώνες δικτύων

Οι αντιπυρικές ζώνες δικτύων σχεδιάζονται για να προστατεύσουν τα δίκτυα από επιθέσεις. Υπάρχουν σε δύο αρχικές μορφές: αφιερωμένη συσκευή (dedicated appliance) ή μια ακολουθία λογισμικού αντιπυρικών ζωνών που εγκαθίσταται πάνω από ένα λειτουργικό σύστημα. Στα βασισμένα σε συσκευή αντιπυρικές ζωνών δικτύων περιλαμβάνονται τα Cisco PIX, Cisco ASA, Juniper's NetScreen, η αντιπυρικές ζώνες της Nokia και Symantec's Enterprise Firewall. Οι δημοφιλέστερες αντιπυρικές ζώνες βασισμένες στο λογισμικό περιλαμβάνουν τα Check Point's Firewall-1 NG, NGX Firewalls, Microsoft ISA Server, Linux-based IPTables και BSD's packet filter. Το λειτουργικό σύστημα Sun Solaris, στο παρελθόν, είχε ενσωματωμένο το SunScreen enterprise firewall και με την έκδοση Solaris 10 παρέχει το open source IP Filter (IPF) ως εναλλακτική λύση στο SunScreen.

Οι αντιπυρικές ζώνες δικτύων παρέχουν στους οργανισμούς ευελιξία και προστασία. Τα τελευταία χρόνια έχουν ενσωματώσει πολλά νέα

χαρακτηριστικά όπως η ευθύγραμμη ανίχνευση παρείσφρησης και πρόληψη (in--line intrusion detection and prevention). Προσφέρουν επίσης δυνατότητα τερματισμού συνδέσεων για εικονικά ιδιωτικά δίκτυα (VPN). Ένα άλλο χαρακτηριστικό γνώρισμα που έχει εισαχθεί στις αντιπυρικές ζώνες δικτύων είναι η ικανότητα πακέτο-επιθεώρησης. Η αντιπυρική ζώνη μπορεί να προσδιορίσει τις απαιτήσεις κυκλοφορίας όχι μόνο απο την εξέταση της πληροφορίας στο στρώμα 3 και 4 (μοντέλο OSI) αλλά με έρευνα έως το στρώμα εφαρμογής. Μέσω αυτής της διαδικασίας, μια αντιπυρική ζώνη μπορεί να λάβει αποφάσεις για τον τρόπο με τον οποίο θα αντιμετωπίσει καλύτερα την κυκλοφοριακή ροή. Αυτή η εξέλιξη στο σχεδιασμό και τις ικανότητες των αντιπυρικών ζωνών έχει οδηγήσει στην ανάπτυξη ενός νέου προϊόντος αντιπυρικών ζωνών, την ενοποιημένη αντιπυρική ζώνη (integrated firewall).

Το όφελος των ενοποιημένων αντιπυρικών ζωνών είναι ότι απλοποιούν το σχεδιασμό των δικτύων με τη μείωση του αριθμού συσκευών στο δίκτυο, παρέχοντας επίσης και ένα ενιαίο σύστημα διαχώρισης, μειώνοντας με αυτόν τον τρόπο το διαχειριστικό φορτίο στους διαχειριστές δικτύων. Ένα άλλο όφελος είναι το ενδεχομένως χαμηλότερο κόστος της συσκευής εναντία των πολυαρίθμων συσκευών και τους πολλαπλάσιους προμηθευτές. Το σημαντικότερο μειονέκτημα είναι η αποτυχία μιας τέτοιας συσκευής, γεγονός που μπορεί να οδηγήσει σε πολλαπλάσιες εκθέσεις σε κίνδυνο. Επιπλέον, η πολυπλοκότητα της συσκευής μπορεί να οδηγήσει σε δυσκολίες στην ανίχνευση λαθών συνδεσιμότητας (connectivity), λόγω της αλληλεπίδρασης των διαφορετικών δυνατοτήτων της συσκευής και του τρόπου με τον όποιο αυτές οι επιπτώσεις θα επηρεάζουν τις θεμελιώδης λειτουργίες μιας αντιπυρικής ζώνης.

3.3 Τεχνολογίες αντιπυρικών ζωνών

Αυτή η ενότητα παρουσιάζει τις τεχνολογίες που χρησιμοποιούνται στις διάφορες αντιπυρικές ζώνες και τον τρόπο λειτουργίας τους. Αναλύεται ένα ευρύ φάσμα τεχνολογιών αντιπυρικών ζωνών, συμπεριλαμβανομένων των παρακάτω:

1. Προσωπικές αντιπυρικές ζώνες
2. Φίλτρα πακέτων
3. Αντιπυρικές ζώνες μεταφράσεων διευθύνσεων δικτύων (NAT)
4. Αντιπυρικές ζώνες επιπέδου συνόδου (Circuit-level firewalls)
5. Αντιπυρικές ζώνες πληρεξούσιου (Proxy firewalls)
6. Αντιπυρικές ζώνες Stateful
7. Διαφανείς αντιπυρικές ζώνες (Transparent firewalls)
8. Εικονικές αντιπυρικές ζώνες (Virtual firewalls)

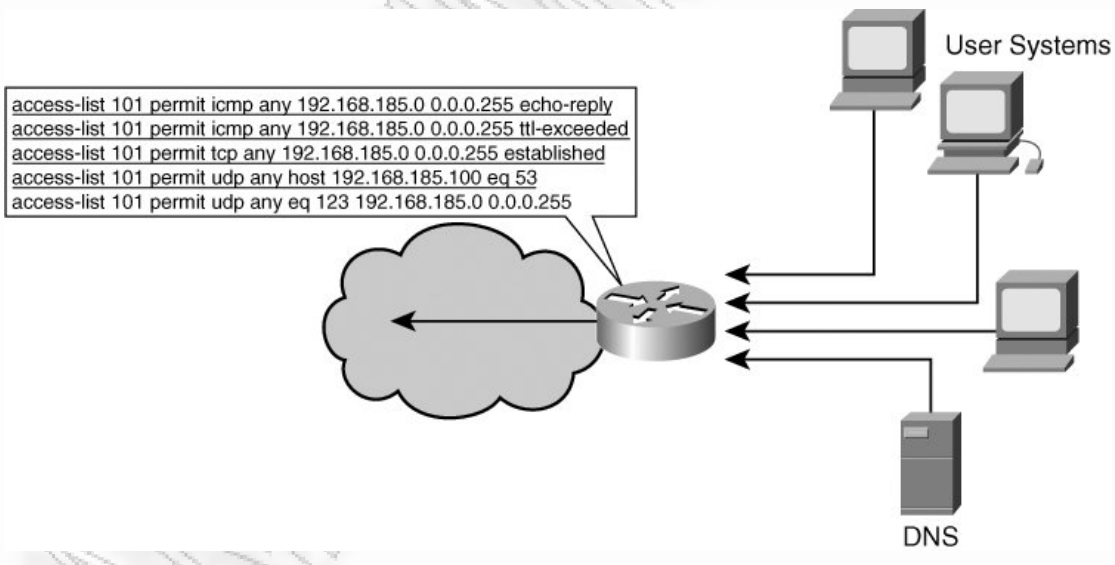
Οι διαφορές τεχνολογίες αντιπυρικών ζωνών μπορούν να χρησιμοποιηθούν σε καθεμία από τις τρεις βασικές φυσικές αντιπυρικές ζώνες (λογισμικού, συσκευής, ή ενοποιημένη).

3.3.1 Προσωπικές αντιπυρικές ζώνες

Οι προσωπικές αντιπυρικές ζώνες σχεδιάζονται για να προστατεύσουν ένα host. Μπορούν να αντιμετωπισθούν ως το περίβλημα προστασίας γύρω από το σύστημα, όπου το σύστημα μπορεί να είναι ένας κεντρικός υπολογιστής, ένας υπολογιστής γραφείου ή ένα laptop. Στις προσωπικές αντιπυρικές ζώνες η εξερχόμενη κυκλοφορία επιτρέπετε ενώ η εισερχόμενη κυκλοφορία απαιτεί επιθεώρηση. Συνήθως οι προσωπικές αντιπυρικές ζώνες περιλαμβάνουν διάφορα προφίλ τα οποία προσαρμόζουν τη κυκλοφορία που θα δεχτεί ένα σύστημα. Ένας σημαντικός παράγοντας είναι η συγκεντρωτική διαχείριση. Το σημαντικότερο εμπόδιο στην επέκταση της προσωπικής αντιπυρικής ζώνης σε κάθε σύστημα είναι η ανάγκη για συγκεντρωτική διαχείριση, έτσι ώστε οι πολιτικές ασφάλειας να μπορούν να αναπτυχθούν και να εφαρμοστούν στα απομακρυσμένα συστήματα. Οι μεγάλες επιχειρήσεις είναι διστακτικές στο να υιοθετήσουν την προσωπική τεχνολογία αντιπυρικών ζωνών για τα συστήματά τους λόγω της δυσκολίας για μια συνεπής πολιτική αντιπυρικών ζωνών σε ολόκληρη την επιχείρηση.

3.3.2 Φίλτρα πακέτων

Τα φίλτρα πακέτων είναι συσκευές δικτύων όπου το φιλτράρισμα της κυκλοφορίας βασίζεται στα απλά χαρακτηριστικά των πακέτων. Θεωρούνται «stateless» δεδομένου ότι δεν κρατούν κάποιο πίνακα κατάστασης σύνδεσης της αντίστοιχης κυκλοφορίας. Για να υπάρξει κυκλοφορία και στις δύο κατευθύνσεις, πρέπει να διαμορφωθούν έτσι ώστε να επιτρέψουν την κυκλοφορία που επιστρέφει. Στα φίλτρα πακέτων ανήκουν τα Cisco IOS access lists καθώς επίσης και το Linux ipfwadm. Αν και τα φίλτρα πακέτων παρέχουν προστασία ενάντια σε μια ευρεία μορφή απειλών, δεν είναι αρκετά δυναμικά ώστε να θεωρηθούν αληθινές αντιπυρικές ζώνες. Το παράδειγμα 3-1 δείχνει μια απλή λίστα έλεγχου πρόσβασης (access list ACL) για το φιλτράρισμα της κυκλοφορίας. Η λίστα είναι βασισμένη στο σχήμα 3-2. Η λίστα έλεγχου εφαρμόζεται στην εισερχόμενη πλευρά της συσκευής φιλτραρίσματος που συνδέει το τοπικό LAN με το Διαδίκτυο.

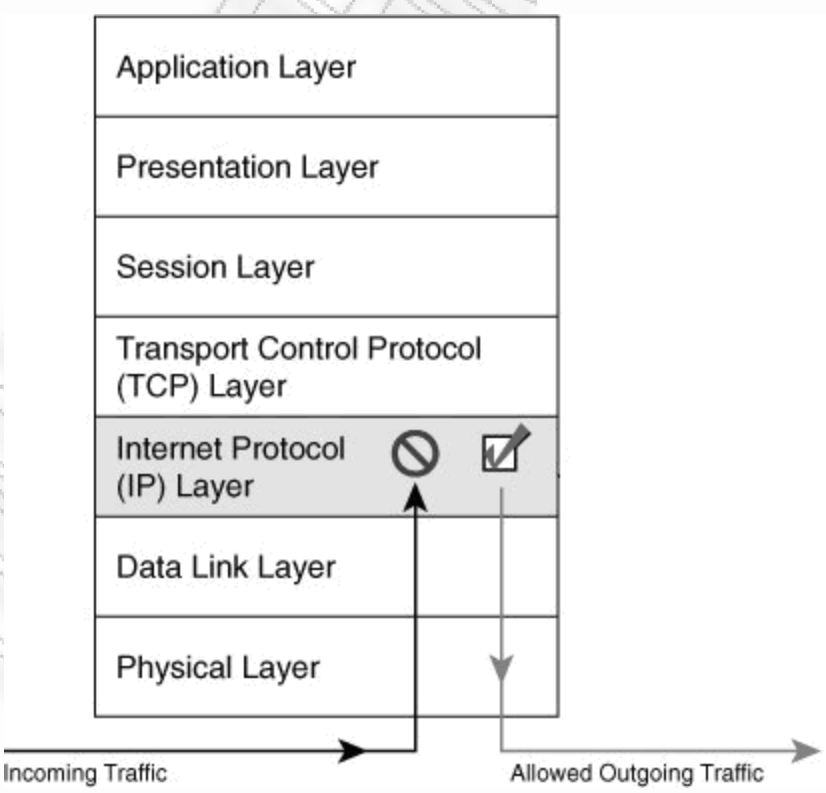


Σχήμα 3-2 : Λίστα έλεγχου πρόσβασης σε μικρό δίκτυο

Παράδειγμα 1-1 : Λίστα έλεγχου πρόσβασης
access-list 101 permit icmp any 192.168.185.0 0.0.0.255 echo-reply
access-list 101 permit icmp any 192.168.185.0 0.0.0.255 ttl-exceeded
access-list 101 permit tcp any 192.168.185.0 0.0.0.255 established
access-list 101 permit udp any host 192.168.185.100 eq 53
access-list 101 permit udp any eq 123 192.168.185.0 0.0.0.255

Ο κανόνας που επιτρέπει την εισερχόμενη κυκλοφορία επιστροφής (inbound return traffic) για dns (53/UDP) και NTP (123/UDP) δηλώνεται ρητά στο τέλος της λίστας. Το ίδιο ισχύει και για τις ICMP echo-reply και time to live (TTL) απαντήσεις. Χωρίς αυτές τις δηλώσεις, αυτά τα πακέτα θα εμποδίζονταν ακόμα και αν ανήκαν σε απάντηση της κυκλοφορίας που δημιουργήθηκε στο προστατευμένο τοπικό LAN. Παρακάτω αναλύεται και ο τρίτος κατά σειρά κανόνας: *access-list 101 permit tcp any 192.168.185.0 0.0.0.255 established.*

Ο κανόνας δημιουργήθηκε για να επιτρέψει την επιστροφή κυκλοφορίας από οποιοδήποτε εξωτερικό σύστημα προς το υποδίκτυο 192.168.185.0/24. Η λέξη κλειδί «established» ορίζει ότι αυτό θα γίνεται μονό όταν η κυκλοφορία επιστροφής έχει ενεργοποιημένη τη σημαία TCP ACK. Συνήθως τα φίλτρα πακέτων δεν έχουν stateful ικανότητες ώστε να επιθεωρήσουν την εξερχόμενη κυκλοφορία και να παραγάγουν δυναμικά τους κανόνες που επιτρέπουν την κυκλοφορία επιστροφής σε μια εξερχόμενη ροή. Το σχήμα 3-3 παρουσιάζει τον τρόπο λειτουργίας μιας απλής αντιπυρικής ζώνης φιλτραρίσματος πακέτων.

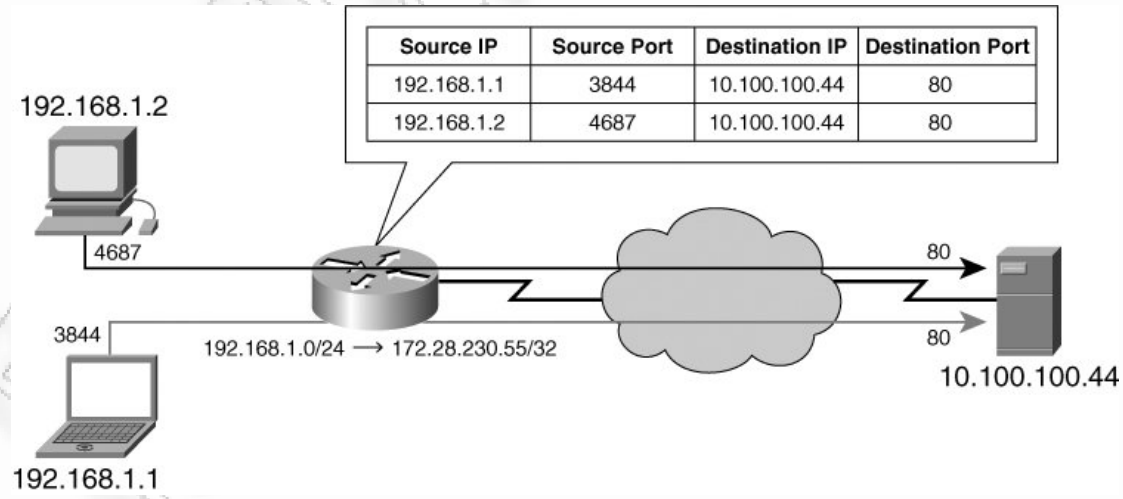


Σχήμα 3-3 : Packet-Filtering Firewall

3.3.3 Αντιπυρικές ζώνες NAT

Μια άλλη αντιπυρική ζώνη, που υπήρξε για μια μικρή χρονική περίοδο, είναι η αντιπυρική ζώνη μεταφράσεων διευθύνσεων δικτύων. Στη σημερινή αγορά η αντιπυρική ζώνη NAT αποτελεί μέρος σχεδόν κάθε διαθέσιμου προϊόντος αντιπυρικών ζωνών. Οι αντιπυρικές ζώνες NAT παρέχουν αυτόματα την προστασία στα συστήματα πίσω από την αντιπυρική ζώνη επειδή επιτρέπουν μόνο τις συνδέσεις που προέρχονται από το εσωτερικό της. Ο βασικός σκοπός του NAT είναι να κάνει πολυπλεξία της κυκλοφορίας στο εσωτερικό δίκτυο ώστε να την παρουσιαστεί στο ευρύτερο δίκτυο (δηλαδή το Διαδίκτυο) σαν να προερχόταν από μια διεύθυνση IP ή μια μικρή σειρά από διευθύνσεις IP.

Η αντιπυρική ζώνη NAT δημιουργεί έναν πίνακα που περιέχει τις πληροφορίες για όλες της συνδέσεις που έχουν δημιουργηθεί. Αυτός ο πίνακας χαρτογραφεί τις διευθύνσεις των εσωτερικών συστημάτων σε μια εξωτερική διεύθυνση. Η δυνατότητα να τοποθετηθεί ένα ολόκληρο δίκτυο πίσω από μια διεύθυνση IP είναι βασισμένη στη χαρτογράφηση των αριθμών θύρας από την NAT αντιπυρική ζώνη. Ένα τέτοιο παράδειγμα χρησιμοποιείται στα συστήματα που παρουσιάζονται στο σχήμα 3-4.



Σχήμα 3-4 : NAT Firewall

Οι hosts στο "εσωτερικό" της αντιπυρικής ζώνης (192.168.1.1 και 192.168.1.2) προσπαθούν να έχουν πρόσβαση στον web server 10.100.100.44. Ο host

192.168.1.1 ανοίγει τη θύρα TCP 3844 και συνδέεται με τον διακομιστή 10.100.100.44 στη θύρα TCP 80. Ο host 192.168.1.2 ανοίγει τη θύρα TCP 4687 και συνδέεται με τον web server 10.100.100.44 στη θύρα TCP 80. Η αντιπυρική ζώνη διαμορφώνεται για να μεταφράσει ολόκληρο το δίκτυο 192.168.1.0/24 στην ενιαία διεύθυνση IP 172.28.230.55. Όταν επεξεργάζεται τις εξερχόμενες συνδέσεις, ξαναγράφει τις πληροφορίες στρώματος IP και αντικαθιστά το 192.168.1.1 και 192.168.1.2 με την ενιαία διεύθυνση IP 172.28.230.55. Εσωτερικά, η αντιπυρική ζώνη διατηρεί έναν πίνακα που παρακολουθεί την κυκλοφορία και μεταφράζει τα 192.168.1.1 και 192.168.1.2 στη διεύθυνση IP 172.28.230.55. Στο παράδειγμα που παρουσιάζεται στο σχήμα 2-4, υπάρχουν δύο μοναδικές υποδοχές (sockets): 192.168.1.1:3844 και 192.168.1.2:4687. Όταν αυτή η κυκλοφορία ελεγχτεί από την αντιπυρική ζώνη, η NAT διαδικασία αντικαθιστά τις 192.168.1 διευθύνσεις με τη 172.28.230.55. Ο πίνακας 3-1 παρουσιάζει την παραπάνω διαδικασία.

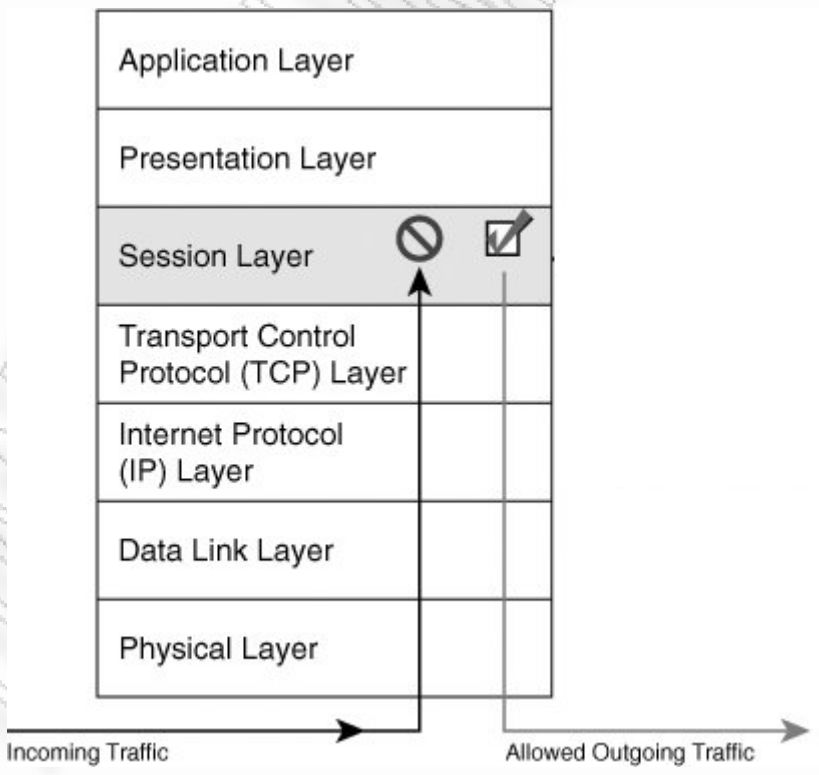
Πίνακας 3-1 : Network Address Translation

Source IP	*Source Port*	*NAT IP*	*NAT port*	*Destination IP*	*Destination Port*
192.168.1.1	3844	172.28.230.55	3844	10.100.100.44	80
192.168.1.2	4687	172.28.230.55	4687	10.100.100.44	80
192.168.1.1	4687	172.28.230.55	63440	10.100.100.44	80

Η τελευταία είσοδος στον πίνακα μας δείχνει την αντίδραση μιας αντιπυρική ζώνης NAT όταν μια συγκεκριμένη θύρα πηγής έχει δεσμευτεί από μια προηγούμενη σύνδεση. Σε αυτήν την περίπτωση, ο client 192.168.1.1 προσπαθεί να κάνει μια δεύτερη σύνδεση στον web server 10.100.100.44. Ο client ανοίγει μια σύνδεση στη θύρα TCP 4687 αλλά αυτή χρησιμοποιείται ήδη από σύνδεση για τον client 192.168.1.2. Σε αυτή την περίπτωση, η NAT αντιπυρική ζώνη αλλάζει όχι μόνο τη διεύθυνση πηγής IP αλλά και τη θύρα πηγής και στην συνεχεία ενημερώνει το πίνακα μεταφράσεών.

3.3.4 Αντιπυρικές ζώνες επιπέδου συνόδου

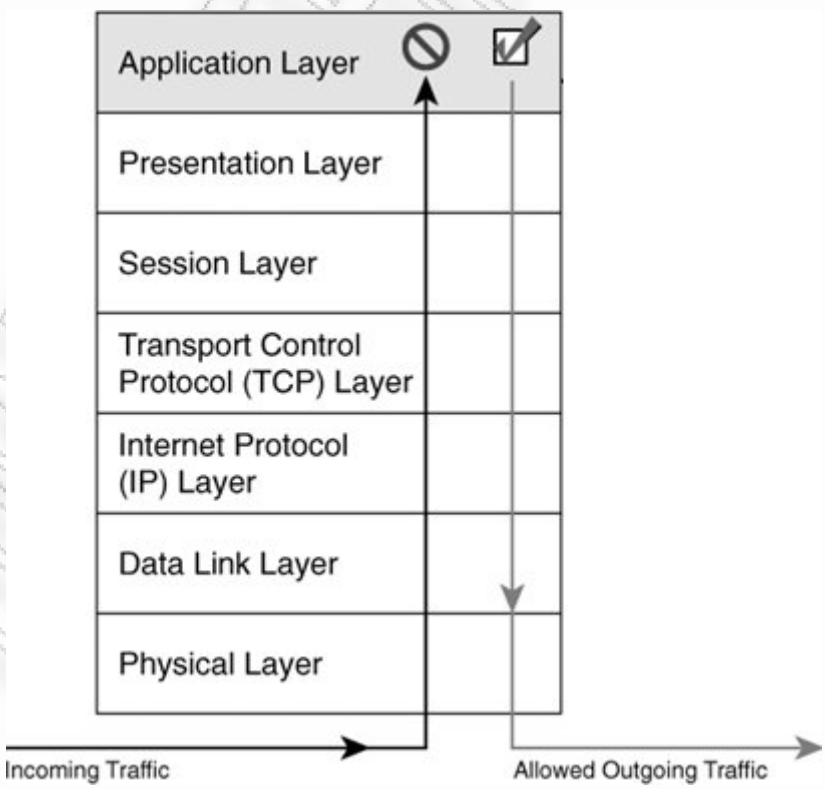
Οι αντιπυρικές ζώνες επιπέδου συνόδου λειτουργούν στο στρώμα συνόδου του μοντέλου OSI. Για να αποφασίσουν εάν η κυκλοφορία είναι νόμιμη, ελέγχουν τις διαδικασίες ανταλλαγείς (handshaking) μεταξύ των πακέτων. Η κυκλοφορία προς έναν απομακρυσμένο υπολογιστή τροποποιείται κατά τέτοιο τρόπο ώστε να εμφανιστεί σαν να προήλθε από την ιδία την αντιπυρική ζώνη. Αυτή η τροποποίηση καθιστά μια αντιπυρική ζώνη επιπέδου συνόδου ιδιαίτερα χρήσιμη στο κρύψιμο των πληροφοριών για ένα προστατευμένο δίκτυο. Το μειονέκτημα της υλοποίησης αντιπυρικής ζώνης επιπέδου συνόδου στέκεται στο γεγονός ότι δεν φιλτράρει τα μεμονωμένα πακέτα σε μια δεδομένη σύνδεση. Το σχήμα 3-5 παρουσιάζει το παράδειγμα μιας αντιπυρικής ζώνης επιπέδου συνόδου, δείχνοντας την εισερχόμενη κυκλοφορία, τον έλεγχο στο επίπεδο συνόδου και την επιτρεπόμενη εξερχόμενη κυκλοφορία.



Σχήμα 3-5 : Circuit-Level Firewall

3.3.5 Αντιπυρικές ζώνες πληρεξούσιου

Μια αντιπυρική ζώνη πληρεξούσιου ενεργεί ως μεσάζων μεταξύ δύο συστημάτων, παρόμοια με τις πύλες επιπέδου συνόδου. Ωστόσο, στην περίπτωση μιας αντιπυρικής ζώνης πληρεξούσιου, η αλληλεπίδραση ελέγχεται στο στρώμα εφαρμογής με τον καταναγκασμό και των δύο πλευρών να διεξάγουν την επικοινωνία μέσω του πληρεξούσιου. Η λειτουργία αυτή επιτυγχάνεται στην αντιπυρική ζώνη με τη δημιουργία και εκτέλεση μιας διαδικασίας που αντανακλά μια υπηρεσία όπως αυτή θα έτρεχε σε ένα απομακρυσμένο σύστημα. Για να υποστηρίξει τις διάφορες υπηρεσίες, η αντιπυρική ζώνη πληρεξούσιου πρέπει να έχει μια υπηρεσία που τρέχει για κάθε πρωτόκολλο: ένα απλό πληρεξούσιο πρωτοκόλλου μεταφορών ταχυδρομείου (SMTP) για το ηλεκτρονικό ταχυδρομείο, ένα πληρεξούσιο πρωτοκόλλου μεταφοράς αρχείων (FTP) για τις μεταφορές αρχείων, και ένα πληρεξούσιο πρωτοκόλλου μεταφοράς υπερκειμένων (HTTP) για τις υπηρεσίες Ιστού. Το σχήμα 3-6 παρουσιάζει το παράδειγμα μιας αντιπυρικής ζώνης πληρεξούσιου.



Σχήμα 3-6 : Proxy Firewall

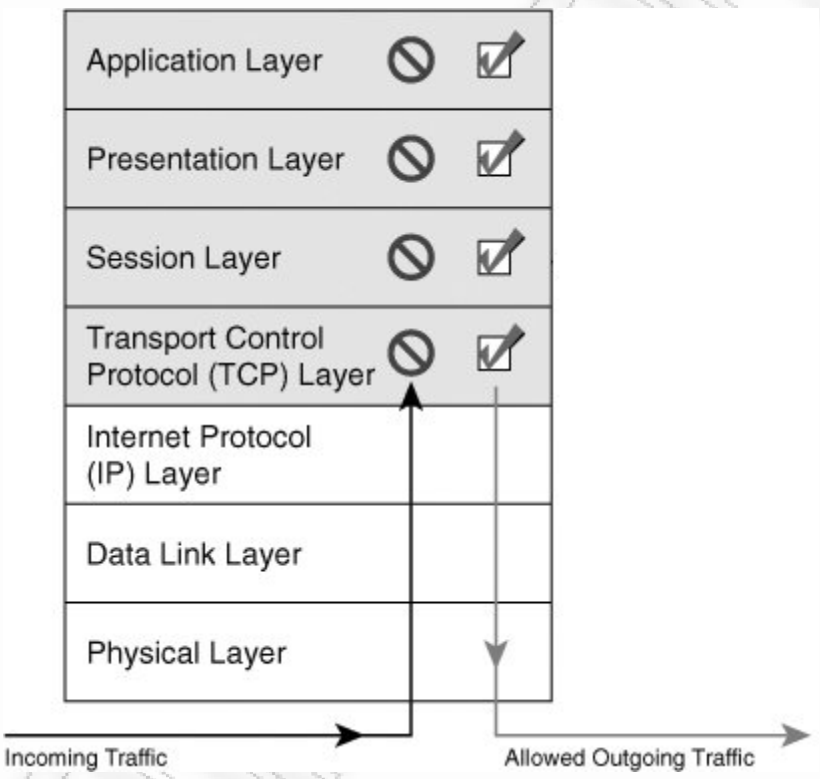
Όταν ένα σύστημα θελήσει να συνδέσει με μια υπηρεσία στο διαδίκτυο, τα πακέτα που περιέχουν το αίτημα σύνδεσης υποβάλλονται σε επεξεργασία από συγκεκριμένη υπηρεσία πληρεξούσιου για το αντίστοιχο πρωτόκολλο και στη συνεχεία δρομολογούνται στο απομακρυσμένο σύστημα. Ομοίως τα πακέτα που επιστρέφουν από τον διακομιστή στο διαδίκτυο, υποβάλλονται σε επεξεργασία από την ίδια υπηρεσία πληρεξούσιου πριν προωθηθούν στο εσωτερικό σύστημα. Εάν δεν υπάρχει καμία δυνατότητα πληρεξούσιου για μια συγκεκριμένη υπηρεσία που τρέχει στην αντιπυρική ζώνη, τότε δεν είναι δυνατή καμία σύνδεση προς τους εξωτερικούς κεντρικούς υπολογιστές που τρέχουν τη συγκεκριμένη υπηρεσία. Σε αυτή την περίπτωση για να φιλτραρίσει τη σύνδεση η αντιπυρική ζώνη μπορεί να χρησιμοποιεί άλλες τεχνολογίες όπως το φιλτράρισμα επιπέδου συνόδου.

Λόγω των ικανοτήτων επιθεώρησής, οι αντιπυρικές ζώνες πληρεξούσιου μπορούν να κάνουν πιο λεπτομερή έλεγχο στα πακέτα μιας σύνδεσης και να εφαρμόσουν πρόσθετους κανόνες ώστε να καθοριστεί εάν ένα πακέτο πρέπει να διαβιβαστεί σε ένα εσωτερικό σύστημα. Η σύνθετη διαμόρφωσή και η ταχύτητά αποτελούν τα μειονεκτήματα μιας αντιπυρικής ζώνης πληρεξούσιου. Επειδή οι αντιπυρικές ζώνες κάνουν αναλυτικό έλεγχο στην εφαρμογή, μπορούν να εισαγάγουν καθυστέρηση στις συνδέσεις δικτύων. Τέλος, εάν για μια ιδιαίτερη εφαρμογή δικτύων δεν υπάρχει καμία συγκεκριμένη υπηρεσία πληρεξούσιου και η εργασία δεν μπορεί να γίνει από μια γενική υπηρεσία πληρεξούσιου, ή εάν η αντιπυρική ζώνη δεν μπορεί να εκτελέσει άλλες μεθόδους, τότε δεν μπορεί να λειτουργήσει πίσω από την αντιπυρική ζώνη.

3.3.6 Αντιπυρικές ζώνες Stateful

Οι σύγχρονες stateful αντιπυρικές ζώνες συνδυάζουν σε ένα σύστημα τις πτυχές και τις ικανότητες των αντιπυρικών ζωνών NAT, επιπέδου συνόδου και πληρεξούσιου. Το φιλτράρισμα της κυκλοφορίας βασίζεται αρχικά στα χαρακτηριστικά των πακέτων αλλά περιλαμβάνει και ελέγχους σε επίπεδο συνόδου για να σιγουρευτεί ότι επιτρέπεται μια συγκεκριμένη σύνοδος.

Αντίθετα από τις άλλες αντιπυρικές ζώνες, σχεδιάζονται για να είναι πιο διάφανης. Ωστόσο, περιλαμβάνουν τις πτυχές φιλτραρίσματος που έχει ένα πληρεξούσιο με το να επιθεωρήσουν ξανά τα στοιχεία σε επίπεδο εφαρμογής, μέσω της χρήσης των συγκεκριμένων υπηρεσιών. Σχεδόν όλες οι σύγχρονες αντιπυρικές ζώνες είναι stateful και αντιπροσωπεύουν τη βασική γραμμή για την ασφάλεια στα σημερινά δίκτυα. Το σχήμα 3-7 απεικονίζει το παράδειγμα μιας αντιπυρικής ζώνης stateful.



Σχήμα 3-7 : Stateful Firewall

3.3.7 Διαφανείς αντιπυρικές ζώνες

Οι διαφανείς αντιπυρικές ζώνες (επίσης γνωστές ως bridging firewalls) δεν είναι μια νέα αντιπυρική ζώνη αλλά μάλλον ένα υποσύνολο των stateful αντιπυρικών ζωνών. Ενώ σχεδόν όλες οι αντιπυρικές ζώνες λειτουργούν στο στρώμα IP και πάνω, οι διαφανείς αντιπυρικές ζώνες λειτουργούν στο δεύτερο στρώμα, το στρώμα ζεύξης δεδομένων (data link layer) και ελέγχουν την κυκλοφορία για τα ανώτερα στρώματα.

Επιπλέον, μια διαφανής αντιπυρική ζώνη μπορεί να εφαρμόσει κανόνες φιλτραρίσματος πακέτων όπως και μια stateful αντιπυρική ζώνη και να εμφανιστεί στον τελικό χρήστη σαν αόρατη. Στην πραγματικότητα, μια διαφανής αντιπυρική ζώνη ενεργεί ως γέφυρα, φιλτράροντας τα πακέτα μεταξύ δύο τμημάτων δικτύου. Αντιπροσωπεύει έναν άριστο τρόπο για εγκατάσταση πολιτικής ασφάλειας στη μέση ενός τμήματος δικτύων, χωρίς να πρέπει να εφαρμοστεί κάποιο φίλτρο NAT. Τα οφέλη των διαφανών αντιπυρικών ζωνών χωρίζονται σε τρεις γενικές κατηγορίες:

- Μηδενική διαμόρφωση (Zero configuration)
- Απόδοση (Performance)
- Μυστικότητα (Stealth)

Η διαφανής αντιπυρική ζώνη δεν απαιτεί καμία τροποποίηση στο υπάρχων δίκτυο, επειδή είναι ευθύγραμμος συνδεδεμένη (in-line plugged) με το δίκτυο που προστατεύει. Επειδή λειτουργεί στο στρώμα ζεύξης δεδομένων, δεν απαιτείται καμία αλλαγή διευθύνσεων IP. Επειδή τείνουν να είναι απλούστερες, έχουν χαμηλότερα φόρτο επεξεργασίας, γεγονός που τις επιτρέπει να παρέχουν την καλύτερη απόδοση καθώς επίσης και τη βαθύτερη επιθεώρηση πακέτων. Τέλος, η μυστικότητά τους προέρχεται άμεσα από το γεγονός ότι είναι συσκευές που λειτουργούν στο δεύτερο στρώμα. Οι διεπαφές δικτύων δεν έχουν καμία διεύθυνση IP (εκτός από τη διεπαφή διαχείρισης) και επομένως είναι αόρατες σε έναν επιτιθέμενο. Δεν μπορεί κάποιος να επιτεθεί επειδή εναντίον της, γιατί απλά δεν μπορεί να την προσεγγίσει.

3.3.8 Εικονικές αντιπυρικές ζώνες

Οι εικονικές αντιπυρικές ζώνες είναι πολλές λογικές αντιπυρικές ζώνες που τρέχουν σε μια ενιαία φυσική συσκευή. Αυτή η ρύθμιση επιτρέπει σε πολλά δίκτυα να προστατεύονται από μια μοναδική αντιπυρική ζώνη που τρέχει μια μοναδική πολιτική ασφάλειας σε μια φυσική συσκευή. Ένας φορέας υπηρεσιών (service provider) μπορεί να παρέχει υπηρεσίες αντιπυρικών ζωνών σε πολλούς

πελάτες, ασφαλίζοντας και διαχωρίζοντας την κυκλοφορία, ενώ η διαχώριση θα γίνεται σε μια συσκευή. Αυτό υλοποιείται με την δημιουργία ξεχωριστών περιοχών ασφάλειας για κάθε πελάτη, όπου κάθε περιοχή θα ελέγχεται από μια διαφορετική λογική εικονική αντιπυρική ζώνη.

3.4 Αντιπυρικές ζώνες ανοικτού και κλειστού κώδικα

Μια άλλη κατηγοριοποίηση που μπορεί να γίνει είναι σε αντιπυρικές ζώνες ανοικτού και κλειστού κώδικα (Open and Closed Source Firewalls). Στις ανοιχτού κώδικα ανήκουν οι Linux's IPTables, OpenBSD's pf, και Solaris IPF. Άλλες, όπως τα Cisco PIX, ASA, Juniper's ScreenOS, Check Point's firewall είναι κλειστού κώδικα. Οι περισσότερες εμπορικές αντιπυρικές ζώνες επιτρέπουν δυνατότητες VPN για τους απομακρυσμένους χρήστες καθώς επίσης και επιθεώρηση πακέτων μέσα στην ίδια αντιπυρική ζώνη. Οι αντιπυρικές ζώνες ανοικτού κώδικα τείνουν να εστιάσουν στις ικανότητες φιλτραρίσματος παρά την ενσωμάτωση άλλων εφαρμογών.

ΚΕΦΑΛΑΙΟ 4

Τοπολογίες και αρχιτεκτονικές αντιπυρικών ζωνών

4.1 Εισαγωγή

Για να είναι μια αντιπυρική ζώνη σε θέση να προστατεύσει επιτυχώς τους πόρους ενός οργανισμού, είναι σημαντικό να εφαρμοστεί καποιος σχεδιασμός που θα αποφέρει προστασία στους πόρους με τον αποδοτικότερο τρόπο. Ο σχεδιασμός θα πρέπει να αποφασιστεί προτού διαμορφωθεί η ίδια η αντιπυρική ζώνη. Κάθε αντιπυρική ζώνη που τοποθετείται μπροστά από τους πόρους παρέχει κάποιο βαθμό προστασίας. Εάν εφαρμοστεί ένα σχέδιο που θα βασίζεται στον τρόπο με τον οποίο οι πόροι πρέπει να προστατευθούν και στη μέθοδο που λειτουργεί η ίδια η αντιπυρική ζώνη, θα είναι πολύ ευκολότερο να εξασφαλιστεί ότι οι πόροι προστατεύονται με μεγαλύτερη ασφάλεια. Θα πρέπει να εφαρμοστεί ένας σχεδιασμός που θα τοποθετεί την αντιπυρική ζώνη στην πιο στρατηγική και αποτελεσματική θέση. Το κεφαλαίο αυτό εξετάζει ζητήματα σχεδιασμού, αρχιτεκτονικής και τις τοπολογίες εγκατάστασης μιας αντιπυρικής ζώνης στο δίκτυο.

4.2 Διαφορετικοί τύποι απαιτήσεων

Αν και η κάθε ανάπτυξη αντιπυρικών ζωνών είναι μοναδική, υπάρχουν μερικά θεμελιώδη σχέδια από τα οποία δημιουργούνται οι περισσότεροι σχεδιασμοί αντιπυρικών ζωνών. Η πρώτη ερώτηση που θα πρέπει να τίθεται κάθε φορά κατά την εφαρμογή μιας αντιπυρικής ζώνης είναι εάν η αντιπυρική ζώνη θα βρίσκεται σε μια κεντρική ή απομακρυσμένη θέση. Για να απαντηθεί η ερώτηση, πρέπει να εξετάσουμε τους πόρους που πρέπει να προστατευθούν. Το επόμενο βήμα είναι να καθοριστεί πόσες αποστρατικοποιημένες ζώνες (DMZs) θα πρέπει να εφαρμοστούν. Αν και οι περισσότερες από αυτές τις ερωτήσεις σχεδιασμού βασίζονται στην προστασία των εσωτερικών πόρων, θα πρέπει να

εφαρμοστούν αντίστοιχα και στη μέθοδο που η αντιπυρική ζώνη θα καλύψει την πρόσβαση στο διαδίκτυο για τους εσωτερικούς πόρους. Προστατεύοντας ουσιαστικά το διαδίκτυο από τα συστήματά μας και επιτρέποντας συγχρόνως το φιλτράρισμα και περιορισμό της κυκλοφορίας που θα επιτραπεί από τους εσωτερικούς πόρους προς το διαδίκτυο.

Κεντρικό γραφείο: Αν και έχει επικράτηση ο ορισμός υλοποίηση κεντρικών γραφείων (central office), δεν είναι απαραίτητο ότι θα πρέπει να υπάρχει ένα κεντρικό γραφείο. Η υλοποίηση κεντρικών γραφείων αναφέρεται περισσότερο σε μια υλοποίηση που έχει διάφορα κοινά στοιχεία:

- Μια συγκέντρωση πόρων που πρέπει να προστατεύουν από την αντιπυρική ζώνη.
- Ένας σημαντικός αριθμός εσωτερικών χρηστών που χρειάζεται πρόσβαση σε εξωτερικούς πόρους μέσω της αντιπυρικής ζώνης
- Το τεχνικό προσωπικό μπορεί να ελέγξει και να διαχειριστεί ενεργά την αντιπυρική ζώνη επειδή βρίσκονται φυσικά στην ίδια θέση.

Κατά συνέπεια, η υλοποίηση κεντρικών γραφείων ισχύει σε οποιοδήποτε περιβάλλον που ταιριάζει με αυτά τα στοιχεία. Χαρακτηρίζεται από μια υλοποίηση που τείνει να είναι πιο σύνθετη από την υλοποίηση στα απομακρυσμένα γραφεία και να χρησιμοποίει περισσότερο υλικό και λογισμικό για να επιτύχει το στόχο της προστασίας των πώρων. Η υλοποίηση κεντρικών γραφείων συχνά υποστηρίζεται από πιο προηγμένες αντιπυρικές ζώνες όπως Cisco PIX, ASA, NetScreen, Check Point, Microsoft ISA Server, ενώ στα απομακρυσμένα και μικρότερα σημεία χρησιμοποιούνται NAT δρομολογητές ή προϊόντα αντιπυρικών ζωνών SOHO.

Απομακρυσμένο γραφείο: Η υλοποίηση για τα απομακρυσμένα γραφεία τείνει να χαρακτηρίζεται από έναν απλούστερο σχεδιασμό. Σε αντίθεση με το κεντρικό γραφείο, έχουν λιγότερους τεχνικούς πόρους σε σχέση με την πείρα που απαιτείται για να διαχειριστεί και συντηρηθεί αποτελεσματικά μια αντιπυρική ζώνη. Επίσης, τα απομακρυσμένα γραφεία σπάνια έχουν τους

εσωτερικούς πόρους που πρέπει να προσεγγιστούν από άλλες απομακρυσμένες πηγές. Αν και η υλοποίηση των κεντρικών γραφείων τείνει να προστατεύσει συνήθως μεγάλο αριθμό από χρήστες και πόρους, στα απομακρυσμένα γραφεία αναφερόμαστε στην προστασία ενός σχετικά μικρού αριθμού χρηστών και πόρων, συνήθως λιγότεροι από 100. Συνεπώς, για τα απομακρυσμένα γραφεία η υλοποίηση μπορεί να γίνει με τη χρήση αντιπυρικών ζωνών SOHO, όπως Cisco PIX 506E, NetScreen 5, NetScreen 25 και δρομολογητές που υποστηρίζουν λειτουργίες NAT.

4.3 Αρχιτεκτονικές μονής αντιπυρικής ζώνης

Υπάρχουν δύο κυρίαρχες αρχιτεκτονικές αντιπυρικών ζωνών, μονή αντιπυρική ζώνη (single-firewall) και διπλή αντιπυρική ζώνη (dual-firewall). Η αρχιτεκτονική μονής αντιπυρικής ζώνης είναι απλούστερη επειδή στηρίζεται στη χρήση μιας ενιαίας συσκευής η οποία φιλτράρει και ελέγχει τη ροή της κυκλοφορίας. Εάν χρησιμοποιηθεί η αρχιτεκτονική μονής αντιπυρικής ζώνης, τότε μπορούμε να επιλέξουμε τους παρακάτω σχεδιασμούς:

1. Αντιπυρική ζώνη Διαδικτύου με μια DMZ
2. Αντιπυρική ζώνη Διαδικτύου με πολλές DMZs
3. Αντιπυρική ζώνη Διαδίκτυο-διαλογής (χωρίς DMZ)

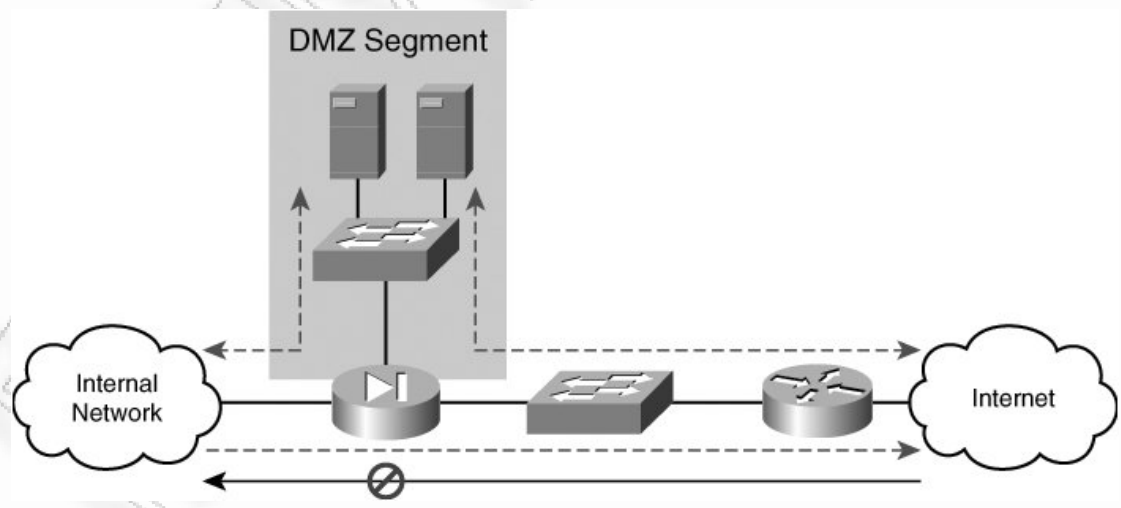
4.3.1 Αντιπυρική ζώνη Διαδικτύου με μια DMZ

Η αντιπυρική ζώνη Διαδικτύου (Internet firewall) με μια αποστρατικοποιημένη ζώνη (De-Militarized Zone – DMZ) είναι η πιο κοινή, επειδή αποτελεί μια αρχιτεκτονική γενικής χρήσης. Συμφώνα με αυτήν την αρχιτεκτονική, η αντιπυρική ζώνη έχει τρεις διεπαφές: μια εσωτερική διεπαφή που συνδέεται με το προστατευμένο δίκτυο, μια εξωτερική διεπαφή που συνδέονται με το διαδίκτυο και μια διεπαφή DMZ που συνδέεται με ένα υποδίκτυο διαλογής

(screened subnet) στο οποίο υπάρχουν οι κεντρικοί υπολογιστές και τα συστήματα που πρέπει να έχουν πρόσβαση οι εξωτερικοί χρήστες.

Στη συγκεκριμένη αρχιτεκτονική, η κυκλοφοριακή ροή ελέγχεται σε τρεις κατευθύνσεις. Η κυκλοφορία που προέρχεται από τα εξωτερικά συστήματα επιτρέπεται μόνο στους πόρους της DMZ. Αυτά τα συστήματα δεν μπορούν ποτέ να έχουν άμεση πρόσβαση σε πόρους στο εσωτερικό δίκτυο. Η κυκλοφορία που προέρχεται από τα συστήματα στη DMZ επιτρέπεται προς το διαδίκτυο καθώς επίσης και προς τους εσωτερικούς πόρους. Με αυτό τον τρόπο, σε περίπτωση που τα δεδομένα που υπάρχουν στο εσωτερικό δίκτυο ζητηθούν από κάποιο εξωτερικό σύστημα, οι πόροι στη DMZ μπορούν συχνά να χρησιμεύσουν ως ένα πληρεξούσιο.

Τέλος, η κυκλοφορία από το εσωτερικό δίκτυο επιτρέπεται και προς στη DMZ και προς το εξωτερικό δίκτυο. Σε όλες τις καταστάσεις, η μόνη κυκλοφορία που πρέπει να επιτραπεί είναι αυτή που επιτρέπεται ρητά από τις λίστες έλεγχου πρόσβασης (ACL). Το σχήμα 4-1 δείχνει την υλοποίηση για μονή αντιπυρική ζώνη με μια DMZ και τους αντίστοιχους περιορισμούς κυκλοφοριακής ροής.



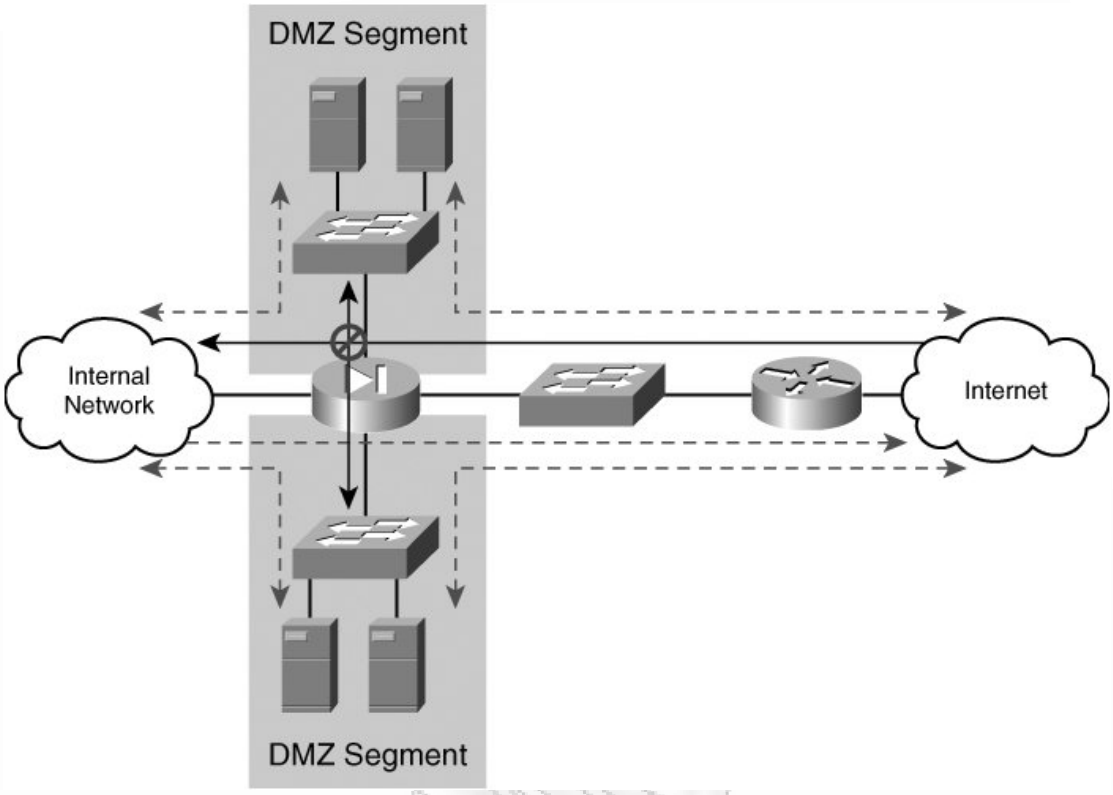
Σχήμα 4-1 : Αντιπυρική ζώνη με μια DMZ

4.3.2 Αντιπυρική ζώνη Διαδικτύου με πολλές DMZ

Η αντιπυρική ζώνη Διαδικτύου με πολλές DMZ είναι παρόμοια με την αρχιτεκτονική για μια DM. Η μόνη πραγματική διαφορά είναι ότι θα υπάρξουν παραπάνω τμήματα DMZ στην αντιπυρική ζώνη. Δεν υπάρχει κανένα πρακτικό όριο στον αριθμό τμημάτων DMZ, ο μόνος πραγματικός περιορισμός είναι ο αριθμός διεπαφών που μπορεί φυσικά ή λογικά να υποστηρίξει η αντιπυρική ζώνη. Αυτή η αρχιτεκτονική εφαρμόζεται όταν υπάρχει η ανάγκη να χωριστούν οι πόροι σε διαφορετικά και ευδιάκριτα τμήματα DMZ. Με μια ενιαία DMZ, όλοι οι πόροι που θα προσεγγιστούν από τις εξωτερικές πηγές συνυπάρχουν στο ίδιο τμήμα DMZ. Αυτό σημαίνει ότι εάν οποιοδήποτε από αυτά τα συστήματα παραβιαστεί, δεν υπάρχει κάτι για να σταματήσει τον επιτιθέμενο από τη χρησιμοποίηση εκείνου του συστήματος ώστε στη συνεχεία να παραβιάσει και τους κρισιμότερους κεντρικούς υπολογιστές σε εκείνο το τμήμα DMZ.

Για να αποφύγουμε μια αντίστοιχη απειλή, μπορούμε να τοποθετήσετε τα συστήματα με διαφορετικές απαιτήσεις ασφάλειας σε ανάλογα τμήματα DMZ, μειώνοντας κατά συνέπεια τη δυνατότητα όπου η παραβίαση ενός ανεξάρτητου συστήματος θα επηρεάσει και τους άλλους πόρους. Παραδείγματος χάριν, μπορούμε να τοποθετήσουμε τους κεντρικούς υπολογιστές δικτύου σε ένα τμήμα DMZ και τους κεντρικούς υπολογιστές SMTP σε ένα διαφορετικό τμήμα DMZ. Εάν παραβιαστούν οι κεντρικοί υπολογιστές δικτύου (που είναι παραδοσιακά πιο ευαίσθητοι στις επιθέσεις), οι κεντρικοί υπολογιστές SMTP θα προστατεύονται ακόμα ακίνδυνα σε ένα άλλο τμήμα DMZ, αφού η αντιπυρική ζώνη δεν επιτρέπει την κυκλοφορία μεταξύ των τμημάτων DMZ.

Όπως και με την αρχιτεκτονική μιας DMZ, θα πρέπει να γίνετε έλεγχος της κυκλοφορίας με τον ίδιο τρόπο ώστε να αποτρέπει όλη την κυκλοφορία από τις εξωτερικές πηγές από το να έχει άμεση πρόσβαση στους εσωτερικούς πόρους. Επίσης πρέπει να απαγορεύετε η κυκλοφορία από ένα τμήμα DMZ σε άλλο. Το σχήμα 4-2 δείχνει μια αρχιτεκτονική αντιπυρικής ζώνης με πολλές DMZ.



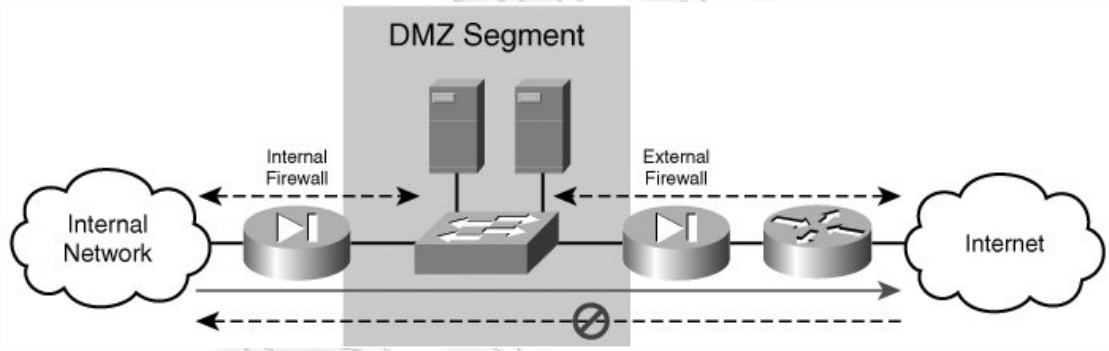
Σχήμα 4-2 : Αντιπυρική ζώνη με δυο DMZ

4.3.3 Αντιπυρική ζώνη χωρίς DMZ

Μια ενιαία αντιπυρική ζώνη χωρίς DMZ μπορεί να λειτουργήσει μονό ως αντιπυρική ζώνη Διαδίκτυο-διαλογής (Internet-screening firewall). Αυτό συμβαίνει επειδή χωρίς τμήμα DMZ, η κυκλοφορία που προέρχεται από το εξωτερικό δίκτυο παραβαίνει το βασικό κανόνα του σχεδιασμού που αναφέρει ότι καμία κυκλοφορία που προέρχεται από μη εμπιστευόμενη πηγή δεν μπορεί άμεσα να έχει πρόσβαση στους εσωτερικούς πόρους. Μια αντιπυρική ζώνη Διαδίκτυο-διαλογής υπάρχει για να κάνει δύο πράγματα. Πρώτον, να αποτρέπει τους εξωτερικούς χρήστες από την έναρξη συνδέσεων προς οποιοδήποτε προστατευμένο πόρο. Δεύτερον, μπορεί να εφαρμοστεί με τέτοιο τρόπο ώστε να φιλτράρει και να περιορίσει την κυκλοφορία από τους εσωτερικούς χρήστες προς τους εξωτερικούς πόρους, όπως για παράδειγμα μέσω της χρήσης λογισμικού φιλτραρίσματος περιεχομένου (content-filtering). Αντίστοιχες αντιπυρικές ζώνες εφαρμόζονται σε απομακρυσμένα σημεία, αφού είναι σπάνιο να περιέχουν πόρους που πρέπει να προσεγγιστούν από εξωτερικές πηγές.

4.4 Αρχιτεκτονική διπλής αντιπυρικής ζώνης

Η αρχιτεκτονική της διπλής αντιπυρικής ζώνης είναι πιο σύνθετη από την αρχιτεκτονική της μιας ενιαίας αντιπυρικής ζώνης, αλλά είναι επίσης και ένας ασφαλέστερος σχεδιασμός. Παρέχει αναλυτικότερο επίπεδο ελέγχου της κυκλοφορίας. Αυτό συμβαίνει επειδή η αρχιτεκτονική χρησιμοποιεί δύο αντιπυρικές ζώνες, διαφορετικών προμηθευτών και προτύπων, που ενεργούν ως εξωτερικές και εσωτερικές αντιπυρικές ζώνες δημιουργώντας μεταξύ τους ένα τμήμα DMZ, όπως φαίνεται και στο σχήμα 4-3. Ομοίως με τους προηγούμενους σχεδιασμούς, επιτρέπεται η κυκλοφορία στο τμήμα DMZ καθώς επίσης και από το εσωτερικό δίκτυο προς στο εξωτερικό δίκτυο, αλλά δεν επιτρέπεται καμία άμεση κυκλοφορία από το εξωτερικό δίκτυο στο εσωτερικό δίκτυο.



Σχήμα 4-3 : Αρχιτεκτονική διπλής αντιπυρικής ζώνης

Ο λεπτομερής έλεγχος σε μια αρχιτεκτονική διπλής αντιπυρικής ζώνης προέρχεται από το γεγονός ότι κάθε αντιπυρική ζώνη ελέγχει ένα υποσύνολο της κυκλοφορίας που εισέρχεται και εξέρχεται από ένα δίκτυο. Επειδή η μη εμπιστευόμενη κυκλοφορία (δηλαδή εξωτερική) δεν πρέπει ποτέ να επιτραπεί να έχει πρόσβαση άμεσα σε ένα εμπιστευμένο (δηλαδή εσωτερικό) δίκτυο, η εξωτερική αντιπυρική ζώνη μπορεί να διαμορφωθεί κατάλληλος για να επιτρέπει την πρόσβαση από το τμήμα DMZ προς τα εξωτερικά συστήματα και αντίθετα. Ομοίως, η εσωτερική αντιπυρική ζώνη μπορεί να διαμορφωθεί ώστε να επιτρέπει την πρόσβαση από το τμήμα DMZ προς τους εσωτερικούς πόρους και αντίθετα. Αυτό επιτρέπει τη δημιουργία δύο ευδιάκριτων και ανεξάρτητων σημείων ελέγχου της κυκλοφορίας από και προς όλα τα τμήματα του δικτυού, είτε αυτά είναι τμήματα DMZ είτε εσωτερικά τμήματα δικτύων.

Όταν μια αρχιτεκτονική διπλής αντιπυρικής ζώνης υλοποιείται με διαφορετικά πρότυπα αντιπυρικών ζωνών (για παράδειγμα, μια αντιπυρική ζώνη Cisco PIX και μια αντιπυρική ζώνη Microsoft ISA Server), κερδίζουμε πρόσθετη ασφάλεια επειδή ένας επιτιθέμενος θα πρέπει να παραβιάσει δύο χωριστές αντιπυρικές ζώνες (που πιθανώς δεν θα είναι ευπαθής στις ίδιες μεθόδους επίθεσης) για να αποκτήσει πρόσβαση στους προστατευμένους πόρους. Επιπλέον, ο επιτιθέμενος πρέπει να είναι γνώστης των δύο διαφορετικών τύπων αντιπυρικών ζωνών για να αλλοιώσει τις διαμορφώσεις τους. Τα μειονεκτήματα μιας αρχιτεκτονικής διπλής αντιπυρικής ζώνης αφορούν την πολυπλοκότητα και το κόστος εφαρμογής. Όσον αφορά την πολυπλοκότητα, μια τέτοια αρχιτεκτονική συχνά απαιτεί να εφαρμόζεται κάποια μορφή δρομολόγησης στο τμήμα DMZ. Η δρομολόγηση χρειάζεται ώστε να επιτρέψει στους πόρους της DMZ να στείλουν την κυκλοφορία που προορίζετε για τα εξωτερικά δίκτυα στην εξωτερική αντιπυρική ζώνη και την κυκλοφορία που προορίζετε για τα εσωτερικά δίκτυα στην εσωτερική αντιπυρική ζώνη.

Αν και οι περισσότεροι οργανισμοί χρησιμοποιούν στατικές δηλώσεις δρομολόγησης στους ιδίους τους κεντρικούς υπολογιστές, όσο μεγαλύτερος είναι ο αριθμός των κεντρικών υπολογιστών στο DMZ, τόσο δυσκολότερος γίνεται το να διαχειριστούν και διατηρηθούν τόσες πολλές δηλώσεις δρομολόγησης. Για τη λύση αυτού του προβλήματος θα μπορούσαν να χρησιμοποιηθούν δρομολογητές, επιτρέποντας στο διαχειριστή να ενημερώνει άμεσα το δρομολογητή με τις νέες διαδρομές. Ωμός η χρήση της δρομολόγησης πρωτοκόλλων πρέπει να αποφευχθεί, επειδή ένας επιτιθέμενος μπορεί να χρησιμοποιήσει τις πληροφορίες που παρέχονται από το πρωτόκολλο δρομολόγησης για να αποκτήσει γνώση σχετικά με την εσωτερική τοπολογία και τη δομή των δικτύων. Εκτός από τις προφανείς δαπάνες σχετικά με την εφαρμογή και τη διατήρηση των πολλών αντιπυρικών ζωνών, η υλοποίηση και διαχείριση μιας αρχιτεκτονική διπλής αντιπυρικής ζώνης είναι ακριβότερη αφού χρειάζεται ανθρώπους με αντίστοιχη τεχνογνωσία. Λόγω του κόστους και της πολυπλοκότητας, η αρχιτεκτονική διπλής αντιπυρικής ζώνης εφαρμόζεται στα περιβάλλοντα με κρίσιμες απαιτήσεις ασφάλειας όπως για παράδειγμα τράπεζες και κυβερνητικούς οργανισμούς.

4.5 Συστήματα αντιπυρικών ζωνών

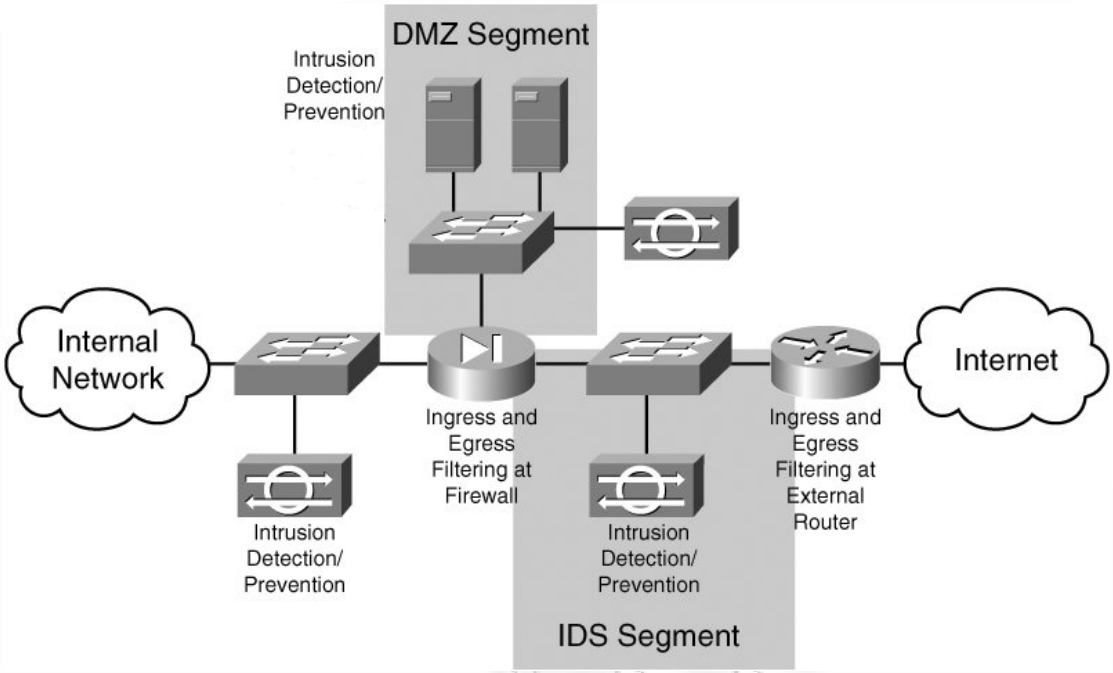
Ιστορικά, μια αντιπυρική ζώνη έχει θεωρηθεί πάντα ως μια συσκευή. Στις περισσότερες περιπτώσεις υπάρχει στην περίμετρο των δικτύων και είναι η μονή αρμόδια για τον έλεγχο της κυκλοφορία που εισέρχεται και εξέρχεται από και προς το προστατευμένο δίκτυο. Αυτή η φιλοσοφία είναι πλέον απαρχαιωμένη και ακατάλληλη. Αντίθετα, μια αντιπυρική ζώνη δεν πρέπει πλέον να θεωρηθεί ως μια συσκευή, αλλά σαν ένα σύστημα συσκευών που λειτουργούν από κοινού για να ελέγξουν τη ροή της κυκλοφορίας από και προς το προστατευμένο δίκτυο. Με βάση τα παραπάνω, το σύστημα αντιπυρικών ζωνών θα πρέπει να εφαρμόζει ένα σχεδιασμό που θα υλοποιείται σε διάφορα στρώματα, αποβάλλοντας την εξάρτηση που επιβάλλει ότι μια συσκευή θα κάνει όλο το φιλτράρισμα. Αυτό επιδρά και στην αποφυγή του ενός μοναδικού σημείου αποτυχίας (single points of failure) που υπάρχει στις παραδοσιακές αρχιτεκτονικές της «μιας συσκευής».

4.5.1 Σύστημα με μια αντιπυρική ζώνη

Στην αρχιτεκτονική μονής αντιπυρικής ζώνης, το σύστημα αντιπυρικών ζωνών αποτελείται από τα ακόλουθα στρώματα:

- Εξωτερικός δρομολογητής
- Τμήμα μεταξύ εξωτερικού δρομολογητή και αντιπυρικής ζώνης
- Τμήμα DMZ

Το σχήμα 4-4 απεικονίζει μια αντίστοιχη αρχιτεκτονική. Στο εξωτερικό στρώμα του συστήματος αντιπυρικών ζωνών, ο εξωτερικός δρομολογητής πρέπει να είναι το πρώτο σημείο ελέγχου της κυκλοφορίας που εισέρχεται και εξέρχεται από το δίκτυό. Η μόνη κυκλοφορία που πρέπει να επιτρέπεται από το δρομολογητή είναι η κυκλοφορία που προορίζεται για την αντιπυρική ζώνη ή τους πόρους που προστατεύεται από την αντιπυρική ζώνη.



Σχήμα 4-4 : Σύστημα με μια αντιπυρική ζώνη

Αυτό εξυπηρετεί δύο σκοπούς. Πρώτον, καθιστά ευκολότερη την παρακολούθηση της κυκλοφορίας στο τμήμα μεταξύ του δρομολογητή και της αντιπυρικής ζώνης. επειδή μόνο η κυκλοφορία που πρέπει να παραδοθεί στην αντιπυρική ζώνη πρέπει να υπάρξει σε εκείνο το τμήμα. Δεύτερον, προστατεύει την αντιπυρική ζώνη από οποιαδήποτε μη επιτρεπτή κυκλοφορία. Κατά συνέπεια μπορεί να εξασφαλίσει ότι εάν για κάποιους λόγους η αντιπυρική ζώνη είναι τρωτή σε μια επίθεση που βασίζεται σε εκείνη την κυκλοφορία, τότε αυτή θα έχει μπλοκαριστεί από το δρομολογητή. Θα πρέπει να λάβουμε υπόψη ότι εκτός από την προστασία της αντιπυρικής ζώνης και των προστατευμένων πόρων, ο ίδιος ο δρομολογητής πρέπει να προστατευθεί για να εξασφαλίσουμε ότι οι εξωτερικές απειλές δεν είναι ικανές να τον στοχεύσουν άμεσα.

Το τμήμα δικτύων μεταξύ του εξωτερικού δρομολογητή και της αντιπυρικής ζώνης είναι το πρώτο σημείο για την εφαρμογή των συστημάτων ανίχνευσης και πρόληψης παρείσφρησης (IDS/IPS). Επειδή μόνο η ρητά επιτρεπόμενη κυκλοφορία πρέπει να διαπέρνα το δρομολογητή, το σύστημα IDS/IPS μπορεί να διαμορφωθεί ώστε να στείλει έναν συναγερμό οποτεδήποτε ανιχνεύει μη επιτρεπτή κυκλοφορία. Η ίδια η αντιπυρική ζώνη είναι το επόμενο στρώμα, και πρέπει να διαμορφωθεί με φίλτρα εισόδου και εξόδου για να επιτρέψει μόνο την

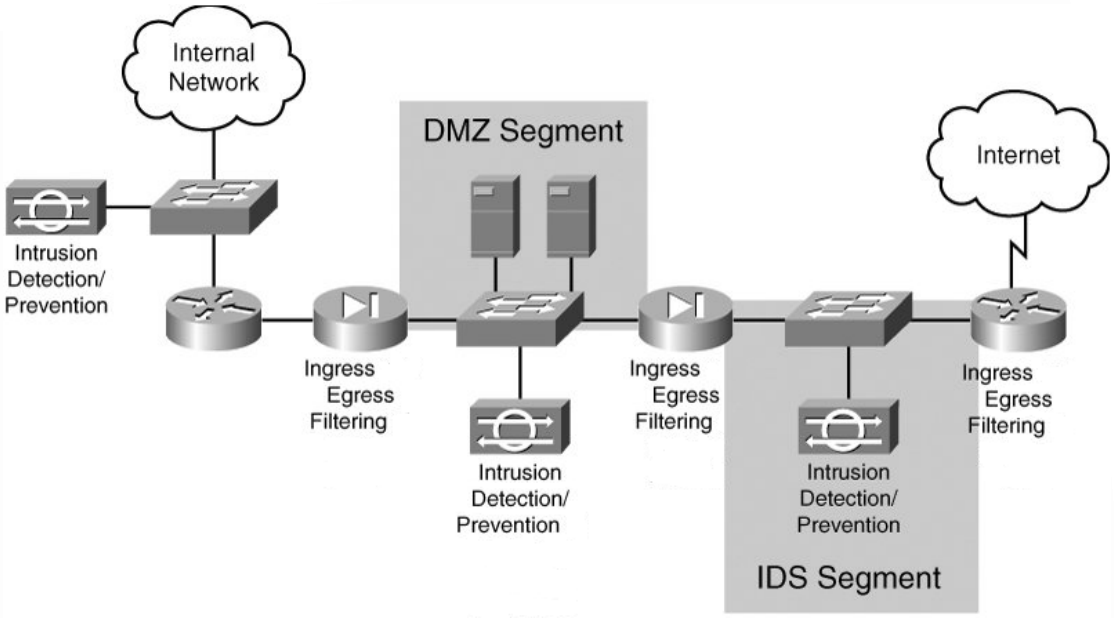
κυκλοφορία που απαιτείται από τους προστατευμένους πόρους, είτε στο DMZ είτε τα εσωτερικά τμήματα δικτύων. Οι πόροι στο τμήμα DMZ πρέπει να προστατευθούν από έναν συνδυασμό αντιπυρικών ζωνών στα ίδια τα συστήματα και IDS/IPS. Μια τέτοια οργάνωση επιτρέπει στο ίδιο το σύστημα να επιτρέψει ή να αρνηθεί, την κυκλοφορία που πρέπει να επιτραπεί. Τέλος, το εσωτερικό δίκτυο προστατεύεται με την προσθήκη φιλτραρίσματος στον εξωτερικό δρομολογητή, την αντιπυρική ζώνη και το IDS/IPS μεταξύ της αντιπυρικής ζώνης και του εσωτερικού δικτύου..

4.5.2 Σύστημα διπλής αντιπυρικής ζώνης

Σε μια αρχιτεκτονική διπλής αντιπυρικής ζώνης, το σύστημα αντιπυρικών ζωνών αποτελείται από τα ακόλουθα στρώματα:

- Εξωτερικός δρομολογητής
- Τμήμα δικτύων μεταξύ εξωτερικού δρομολογητή και εξωτερικής αντιπυρικής ζώνης
- Εξωτερική αντιπυρική ζώνη
- Τμήμα DMZ
- Εσωτερική αντιπυρική ζώνη

Το σχήμα 9-5 απεικονίζει ένα σύστημα διπλής αντιπυρικής ζώνης. Η μόνη πραγματική φυσική διαφορά που έχει το σύστημα διπλής αντιπυρικής ζώνης από το σύστημα μονής αντιπυρικής ζώνης είναι η εφαρμογή δύο αντιπυρικών ζωνών. Αυτή η οργάνωση προβλέπει ξεχωριστά και ευδιάκριτα σημεία επιτήρησης στο δίκτυό για να ελέγξει τη ροή της κυκλοφορίας, με το κατάλληλο φιλτράρισμα εισόδου και εξόδου στις εξωτερικές και εσωτερικές αντιπυρικές ζώνες.



Σχήμα 4-5 : Σύστημα διπλής αντιπυρικής ζώνης

4.6 Εικονικές αντιπυρικές ζώνες και VLAN

Οι εικονικές αντιπυρικές ζώνες (virtual firewalls) βασίζονται στην πρακτική της χρησιμοποίησης εικονικών τοπικών δικτύων (Virtual Local Area Network – VLAN). Εάν μπορούμε να διαχωρίσουμε λογικά έναν μεταγωγέα σε πολλά υποδίκτυα, τότε έχουμε τη δυνατότητα να χρησιμοποιήσουμε μια διεπαφή της αντιπυρικής ζώνης ώστε να κάνει το φιλτράρισμα μεταξύ των λογικών υποδικτύων. Το όφελος αυτής της προσέγγισης είναι η περαιτέρω μειώσει του κόστος υλοποίησης, αφού αφαιρείται η ανάγκης της σύνδεσης κάθε VLAN με μια ξεχωριστή φυσική διεπαφή. Οι εικονικές αντιπυρικές ζώνες δημιουργούνται με το διαχωρισμό μιας ενιαίας αντιπυρικής ζώνης σε πολλαπλάσιες λογικές αντιπυρικές ζώνες, ή αλλιώς πλαίσια ασφάλειας (security contexts). Οι εικονικές αντιπυρικές ζώνες εφαρμόζονται συνήθως σε συσκευές δικτύων που υποστηρίζουν υλικό ή λογισμικό αντιπυρικών ζωνών ως συστατικό της συσκευής. Στη συνεχεία η εικονική αντιπυρική ζώνη μπορεί να συνδεθεί με τα αντίστοιχα VLAN, παρέχοντας την ίδια λειτουργία που θα υπήρχε εάν μια φυσική αντιπυρική ζώνη είχε χρησιμοποιηθεί για να χωρίζει τα VLAN από το υπόλοιπο δίκτυο.

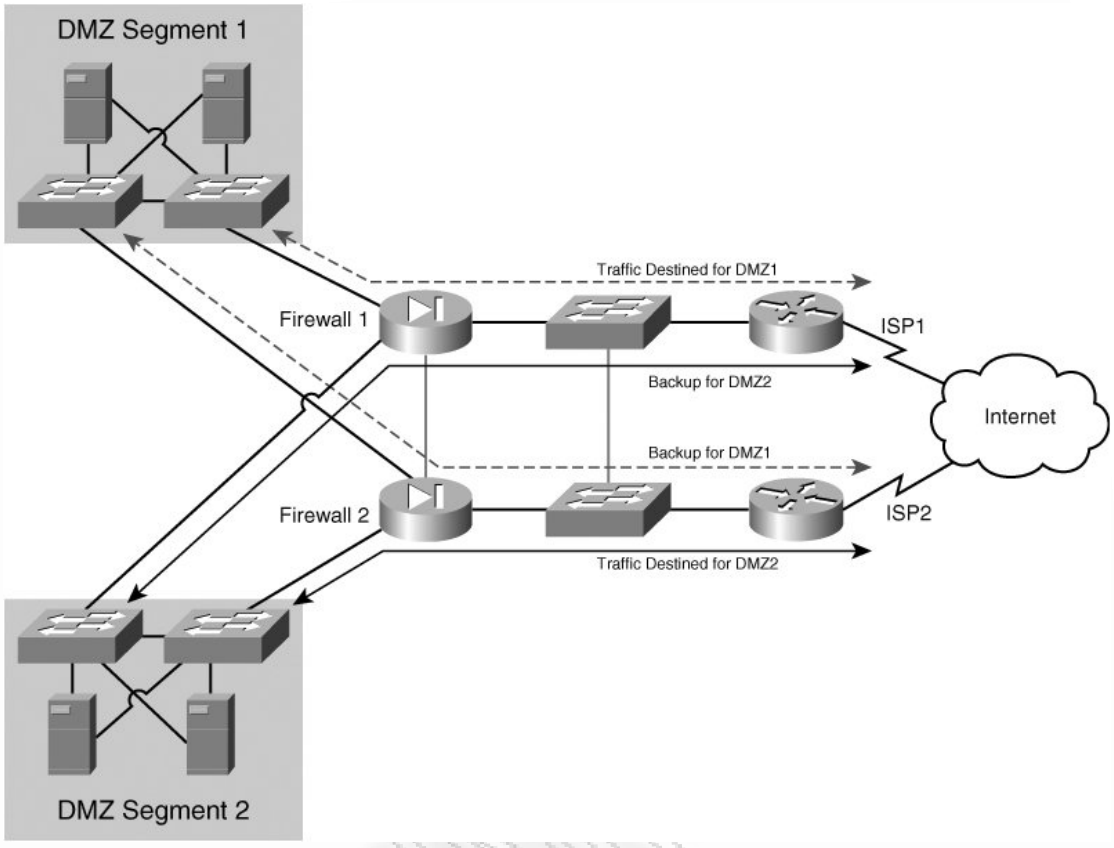
Επειδή οι εικονικές αντιπυρικές ζώνες μπορούν εύκολα να ενσωματωθούν σε πολλούς μεταγωγής, αποτελούν ένα τρόπο διαχωρισμού και προστασίας των εσωτερικών πώρων. Επίσης χρησιμοποιούν τα VLAN ως μέθοδο κατάτμησης για να διαχωρίσουν τα τμήματα DMZ. Ένα μεγάλο μειονέκτημα των εικονικών αντιπυρικών ζωνών είναι το γεγονός ότι χρειάζεται χρόνος για την κατανόηση και διαμόρφωση τους. Αυτό μπορεί να καταστήσει δύσκολη την ανίχνευση λαθών και των εντοπισμό των προβλημάτων. Επιπλέον, κάθε εικονική αντιπυρική ζώνη αντιμετωπίζεται διαχειριστικά ως ξεχωριστή, αυξάνοντας έτσι το κόστος διαχείρισης. Τέλος, σε ορισμένες διαμορφώσεις, οι εικονικές αντιπυρικές ζώνες μπορεί να μην είναι σε θέση να υποστηρίξουν τεχνολογίες όπως τα δυναμικά πρωτόκολλα δρομολόγησης .

4.7 Σχεδιασμός αντιπυρικών ζωνών υψηλής διαθεσιμότητας

Επειδή οι αντιπυρικές ζώνες αποτελούν κρίσιμους κρίκους στην αλυσίδα της υποδομής ενός δικτυού, είναι σημαντικό να εξασφαλιστεί ότι η αντιπυρική ζώνη, και η λειτουργίες που παρέχει, θα είναι πάντα διαθέσιμες και προσιτές. Η υψηλή διαθεσιμότητα και ο πλεονασμός συνήθως αντιμετωπίζονται με τον έναν από τους παρακάτω τρόπους failover:

- Ενεργό / παθητικό (Active / passive failover)
- Ενεργό / ενεργό (Active / active failover)

Ανεξάρτητα από τη μέθοδο, η υψηλή διαθεσιμότητα στηρίζεται στην εφαρμογή δύο αντιπυρικών ζωνών σε μια παράλληλη διαμόρφωση. Στο ενεργό/παθητικό σύστημα, μονό η μια αντιπυρική ζώνη διαχειρίζεται ενεργά την κυκλοφορία ενώ η δεύτερη είναι παθητική και δεν περνά κυκλοφορία. Εάν η ενεργή αντιπυρική ζώνη για οποιοδήποτε λόγο σταματήσει τότε η παθητική αντιπυρική ζώνη γίνεται ενεργή, παρέχοντας τη δυνατότητα στην κυκλοφορία να συνεχίσει να διαβιβάζεται. Σε ένα ενεργό/ενεργό σύστημα, κάθε αντιπυρική ζώνη είναι σε θέση να διαχειρίζεται κυκλοφορία. Το είδος και η ποσότητα της κίνησης καθορίζεται από τα διαφορετικά πλαίσια ασφάλειας.



Σχήμα 4-6 : Παράδειγμα συστήματος active/active failover

Το σχήμα 4-6 παρουσιάζει ένα ενεργό/ενεργό σύστημα. Σε αυτό το παράδειγμα, η κάθε αντιπυρική ζώνη είναι ενεργή για το αντίστοιχο τμήμα DMZ (Firewall1-DMZ1, Firewall2-DMZ2). Εάν για κάποιους λόγους το Firewall2 αποτύχει, η κυκλοφορία που προορίζεται για την DMZ2 θα δρομολογηθεί στο Firewall1, το οποίο με τη σειρά του θα την παραδώσει στην DMZ2. Είναι σημαντικό να σημειώσουμε ότι σε μια τέτοια διαμόρφωση, οι αντιπυρικές ζώνες δεν μπορούν να περάσουν ταυτόχρονα την ίδια κυκλοφορία. Για παράδειγμα, τα Firewall1 και Firewall2 δεν μπορούν να είναι ταυτόχρονα αρμόδιοι για τους ιδίους κανόνες (ruleset) που επιτρέπουν την κυκλοφορία στο ίδιο τμήμα DMZ. Η πρώτη αντιπυρική ζώνη (primary) θα χειρίζεται όλη την κυκλοφορία της DMZ1 και η άλλη αντιπυρική ζώνη θα είναι δευτερεύουσα (secondary). Το πλεονέκτημα μιας ενεργού/ενεργού διαμόρφωσης είναι ότι χρησιμοποιείται όλος ο εξοπλισμός, περεχώντας δυνατότητες εξισορροπήσεις φορτιού (load balancing) μοιράζοντας την κίνηση στις αντιπυρικές ζώνες.

ΚΕΦΑΛΑΙΟ 5

Βασική διαμόρφωση αντιπυρικής ζώνης

5.1 Εισαγωγή

Οι συσκευές ασφάλειας PIX και ASA αποτελούν τις λύσεις που προσφέρει η εταιρία Cisco στην τεχνολογία των αντιπυρικών ζωνών. Είναι ένα κρίσιμο και κύριο συστατικό στην ασφάλεια των δικτύων. Και οι δυο συσκευές επιδέχονται τον ίδιο τρόπο διαμόρφωσης και υποστηρίζουν σχεδόν τις ίδιες τεχνολογίες. Πρακτικά, η δυναμική συσκευή ασφάλειας ASA (Adaptive Security Appliance) είναι η νέα γενιά των PIX. Ο προγραμματισμός και η διαμόρφωση τους, ώστε να υλοποιηθούν στις διάφορες τοπολογίες δικτύων, μπορεί να γίνει με πολλούς τρόπους. Ωστόσο, ο κατάλληλος και σωστός προγραμματισμός είναι απαραίτητος για μια πετυχημένη υλοποίηση των γνωρισμάτων ασφάλειας (security features) που προσφέρουν. Ο σκοπός αυτού του κεφαλαίου είναι να κάνει μια εισαγωγή στη διαμόρφωση των συσκευών ασφάλειας. Το κεφαλαίο αρχίζει με την περιγραφή του τρόπου πρόσβασης στη συσκευή ασφάλειας και στη συνεχεία παρουσιάζει τις βασικές εντολές που απαιτούνται για να διαμορφώσουν και να παρακολουθήσουν μια συσκευή ασφάλειας.

5.2 Τρόποι πρόσβασης

Η συσκευή ασφάλειας παρέχει δύο τύπους διεπαφής χρήστη :

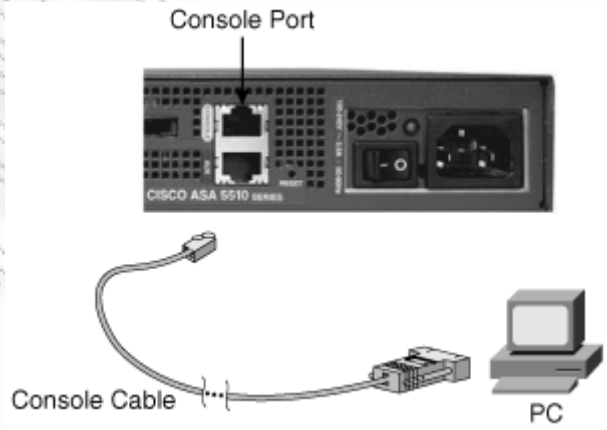
- Διεπαφή γραμμής εντολών - Command line interface (CLI)
- Γραφική διεπαφή χρήστη - Graphical user interface (GUI)

Το CLI παρέχει μη γραφική πρόσβαση και μπορεί να προσεγγιστεί από μια κονσόλα, Telnet, ή Secure Shell (SSH) σύνοδο. Το GUI περιβάλλον μπορεί να χρησιμοποιηθεί μέσω του Adaptive Security Device Manager (ASDM).

Εγκατάσταση σύνδεσης μέσω κονσόλας: Μια νέα συσκευή ασφάλειας, δεν έχει καμία διεύθυνση IP στις διεπαφές της. Για να ολοκληρωθεί η πρόσβαση μέσω CLI, θα πρέπει να υπάρχει σύνδεση στη θύρα κονσόλας (console port) της συσκευής ασφάλειας. Η θύρα κονσόλας είναι μια σειριακή ασύγχρονη θύρα με τα χαρακτηρίστηκα που αναφέρονται στον πίνακα 5-1.

Πίνακας 5-1 : Ρυθμίσεις κονσόλας	
Παράμετρος	*Τιμή*
Baud rate	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware

Η θύρα κονσόλας μπορεί να συνδεθεί με μια σειριακή θύρα του υπολογιστή χρησιμοποιώντας ένα καλώδιο κονσόλας, με έναν DB9 σειριακό προσαρμογέα στη μια άκρη και RJ-45 στην άλλη. Η DB9 πλευρά του καλωδίου πηγαίνει στην σειριακή θύρα του υπολογιστή, ενώ το RJ-45 πηγαίνει στη θύρα κονσόλας της συσκευής ασφάλειας, όπως δείχνει και το σχήμα 5-1.



Σχήμα 5-1 : Σύνδεση μέσω κονσόλας

Αφού συνδεθεί το καλώδιο κονσόλας με τη συσκευή ασφάλειας και τον υπολογιστή, τότε μπορούμε να χρησιμοποιήσουμε κάποιο λογισμικό όπως το HyperTerminal ή το TeraTerm. Σε ένα υπολογιστή με λειτουργικό σύστημα Windows μπορούμε για να ανοίξουμε το HyperTerminal ακλουθώντας τη διαδρομή Start > Programs > Accessories > Communications > HyperTerminal.

5.3 Διεπαφή χρήστη

Οι συσκευές ασφάλειας περιέχουν ένα σύνολο εντολών βασισμένο στο Λειτουργικό Σύστημα Διαδικτύου (Internetwork Operating System – IOS) και παρέχουν τέσσερις τρόπους πρόσβασης:

- **Μη προνομιακή κατάσταση** (unprivileged mode): Διαθέσιμη κατά την αρχική πρόσβαση στη συσκευή ασφάλειας. Εμφανίζει το σύμβολο υπαγόρευσης >. Αυτή η κατάσταση παρέχει μια περιορισμένη εικόνα (restricted view) των ρυθμίσεων.
- **Προνομιακή κατάσταση** (privileged mode): Εμφανίζει το σύμβολο υπαγόρευσης # και επιτρέπει αλλαγές στις τρέχουσες ρυθμίσεις.
- **Κατάσταση διαμόρφωσης** (configuration mode): Εμφανίζει την υπαγόρευση (config)# και επιτρέπει αλλαγές στη διαμόρφωση του συστήματος. Υποστηρίζει και τις εντολές που περιέχονται στις δυο παραπάνω καταστάσεις.
- **Κατάσταση ελέγχου** (monitor mode)**:** Είναι μια ειδική κατάσταση που επιτρέπει την αναβάθμιση του λειτουργικού πάνω από το δίκτυο και την αποκατάσταση κωδικού πρόσβασης (password recovery).

Μέσα σε κάθε τρόπο πρόσβασης, μπορούμε να συντομεύουμε τις περισσότερες εντολές χρησιμοποιώντας τους μοναδικούς χαρακτήρες τις κάθε εντολής. Για παράδειγμα, μπορούμε να χρησιμοποιήσουμε το *sh run* για να δούμε τη διαμόρφωση αντί της πλήρους εντολής *show running-config*.

Πρόσβαση στην προνομιακή κατάσταση: Για να ξεκινήσουμε το προγραμματισμό σε μια συσκευή ασφάλειας, η πρώτη εντολή που πρέπει να γνωρίζουμε είναι η *enable*, που μας παρέχει την είσοδο στην προνομιακή κατάσταση. Όταν η συσκευή περιέχει τις εργοστασιακές ρυθμίσεις δεν απαιτείται κωδικός πρόσβασης. Μπορούμε απλά να πιέσουμε *Enter* στην υπαγόρευση κωδικού πρόσβασης ή να δημιουργήσουμε έναν κωδικό πρόσβασης της επιλογής μας. Όπως φαίνεται και στο παράδειγμα 5-1, όταν εισέρθουμε στην προνομιακή κατάσταση η υπαγόρευση θα αλλάξει σε #.

Παράδειγμα 5-1 : Πρόσβαση στην προνομιακή κατάσταση
pixfirewall> enable password: pixfirewall#

Πρόσβαση στην κατάσταση διαμόρφωσης: Για να μεταφερθούμε από την προνομιακή στην κατάσταση διαμόρφωσης χρησιμοποιούμε την εντολή *configure terminal*. Όπως δείχνει και το παράδειγμα 5-2, μόλις εισάγουμε την εντολή, η υπαγόρευση αλλάζει σε *(config)#.* Για να επιστρέψουμε στην προηγούμενη κατάσταση κάνουμε χρήση των εντολών *exit, end, quit*.

Παράδειγμα 5-2 : Πρόσβαση στην κατάσταση διαμόρφωσης
pixfirewall# configure terminal pixfirewall(config)# exit pixfirewall# exit pixfirewall>

Εντολή βοήθειας *help*: Οι πληροφορίες βοήθειας είναι διαθέσιμες μέσω της διεπαφής γραμμής εντολών CLI. Εάν εισάγουμε την εντολή *help* και μετά το σύμβολο *?* τότε εμφανίζονται οι διαθέσιμες εντολές στο τρέχον επίπεδο.

Παράδειγμα 5-3 : Εντολή *help*
pixfirewall > help ? enable Turn on privileged commands exit Exit the current command mode

login Log in as a particular user
logout Exit from current command mode, and to unprivileged mode
quit Exit the current command mode

pixfirewall > help enable
USAGE:
enable [<priv_level>]
DESCRIPTION:
enable Turn on privileged commands

5.4 Διαχείριση αρχείων

Παρακάτω περιγράφεται το σύστημα διαχείρισης αρχείων στη συσκευή ασφάλειας. Υπάρχουν δύο μνήμες διαμόρφωσης, αυτή που εκτελείται εκείνη τι στιγμή και ονομάζεται τρέχουσα διαμόρφωση (running configuration) και η αρχική ή αλλιώς διαμόρφωση ξεκινήματος (startup configuration). Οι εντολές που περιέχονται στο παράδειγμα 5-4 μας επιτρέπουν να διαβάσουμε ή να αποθηκεύσομε τη διαμόρφωσή:

Παράδειγμα 5-4 : Εντολές διαχείρισης αρχείων
copy run start
show running-config
show startup-config
write memory
write terminal

Η εντολή *show running-config* εμφανίζει στο τερματικό την τρέχουσα διαμόρφωση που υπάρχει στη μνήμη RAM. Όλες οι αλλαγές που γίνονται στη διαμόρφωση «γράφονται» στην τρέχουσα διαμόρφωση. Η μνήμη αυτή δεν είναι μόνιμη και εάν η συσκευή ασφάλειας χάσει την παροχή ρεύματος ή κάνει επανεκκίνηση, όλες οι αλλαγές της τρέχουσας διαμόρφωσης που δεν έχον προηγουμένως αποθηκευτή θα χαθούν. Οι εντολές *copy run start* και *write*

memory αποθηκευθούν την τρέχουσα διαμόρφωση στη διαμόρφωση ξεκινήματος. Η τελευταία χρησιμοποίει ως μέσο αποθήκευσης την μόνιμη μνήμη Flash. Όταν η διαμόρφωση αποθηκεύεται στη μνήμη Flash, μπορούμε να την προβάλλουμε με χρησιμοποίηση της εντολής *show startup-config* ή της *show configure***.**

Καθαρισμός τρέχουσας διαμόρφωσης: Η εντολή *clear config all* «καθαρίζει» την τρέχουσα διαμόρφωση. Όταν την εκτελεσουμε, η τρέχουσα διαμόρφωση χάνεται και επανέρχεται στην διαμόρφωση προεπιλογής (default running configuration).

Παράδειγμα 5-5 : Καθαρισμός τρέχουσας διαμόρφωσης
fw1(config)# clear config all

Διαγράφει αρχικής διαμόρφωσης: Η εντολή *write erase* διαγράφει την αρχική διαμόρφωση και μετά από επανεκκίνηση η συσκευή ασφάλειας επανέρχεται στη διαμόρφωση προεπιλογής. Για να αντιγράψουμε την τρέχουσα διαμόρφωση στη μνήμη Flash πληκτρολογούμε την εντολή *copy run start*.

Παράδειγμα 5-6 : Καθαρισμός αρχικής διαμόρφωσης
fw1# write erase

Επανεκκίνηση συσκευής: Η εντολή *reload,* που παρατίθεται στο παράδειγμα 5-7, μας παρέχει την δυνατότητα επανεκκίνησης της συσκευής ασφάλειας και είναι αλληλεπιδραστική (interactive). Ελέγχει πρώτα εάν η διαμόρφωση έχει τροποποιηθεί και δεν έχει αποθηκευτεί και σε αυτή την περίπτωση, προτρέπει για αποθήκευση της διαμόρφωσης. Αμέσως μετά αρχίζει η διαδικασία επανεκκίνησης, εκτός και αν έχουμε ορίσει κάποια παράμετρο καθυστέρησης. Για να ακυρωθεί μια σχεδιασμένη επανεκκίνηση χρησιμοποιούμε την εντολή *reload cancel*. Στην περίπτωση που είναι ήδη υπό εξέλιξη δεν μπορεί να ακυρωθεί. Εάν θελήσουμε να επαναφέρουμε τη συσκευή ασφάλειας πίσω σε μια διαμόρφωση προεπιλογής, εκτελούμε τις εντολές the *write erase* και *reload*.

Παράδειγμα 5-7 : Επανεκκίνηση συσκευής
fw1# reload Proceed with reload?[confirm] y Rebooting...

Εμφάνιση αποθηκευμένων αρχείων: Για τον έλεγχο των περιεχόμενων καταλόγου (directory contents), εκτελούμε την εντολή *dir* στην προνομιακή κατάσταση EXEC. Η εντολή *dir* χωρίς τις λέξεις κλειδιά εμφανίζει το περιεχόμενο του τρέχοντος καταλόγου. Στο παράδειγμα 5-8, τα αρχεία λογισμικού asdm-501.bin και pix-701.bin είναι αποθηκευμένα στη flash. Η εντολή εμφανίζει επίσης και το υπόλοιπο της ελεύθερης μνήμης που είναι διαθέσιμη.

Παράδειγμα 5-8 : Εμφάνιση αποθηκευμένων αρχείων
fw1# dir Directory of flash:/ 3 -rw- 4902912 13:37:33 Jul 27 2005 pix-701.bin 4 -rw- 6748932 13:21:13 Jul 28 2005 asdm-501.bin 16128000 bytes total (4472832 bytes free)

Επιλογή αρχείου εκκίνησης συστήματος: Για να διευκρινιστεί το αρχείο λογισμικού (image) ή διαμόρφωσης (configuration) που θα χρησιμοποιήσει το σύστημα στην επόμενη επανεκκίνηση, μπορεί να χρησιμοποιηθεί η εντολή *boot* στην προνομιακή κατάσταση EXEC. Μπορούμε να εισάγουμε μέχρι τέσσερις εντολές *boot system***.**

Παράδειγμα 5-9 : Επιλογή αρχείου εκκίνησης συστήματος
fw1(config)# boot system flash:/pix-701.bin

Επαλήθευση συστήματος εκκίνησης : Για να εμφανίσουμε τα αρχεία εκκίνησης, χρησιμοποιήστε στη προνομιακή κατάσταση την εντολή **show boot**. Στο παράδειγμα 5-10, δίνεται η έξοδος της εντολής. Στην περίπτωση μας, το λειτουργικό εκκίνησης θα είναι το 701.bin.

Παράδειγμα 5-10 : Επαλήθευση συστήματος εκκίνησης
fw1# show bootvar BOOT variable = flash:/pix-701.bin Current BOOT variable = flash:/pix-701.bin CONFIG_FILE variable = Current CONFIG_FILE variable =

5.5 Αλγόριθμος και επίπεδα ασφάλειας

Παρακάτω αναλύονται οι λειτουργίες που εκτελεί ο αλγόριθμος ασφάλειας (security algorithm) και τα επίπεδα ασφάλειας (security levels) που μπορεί να διαμορφωθούν σε μια συσκευή ασφάλειας.

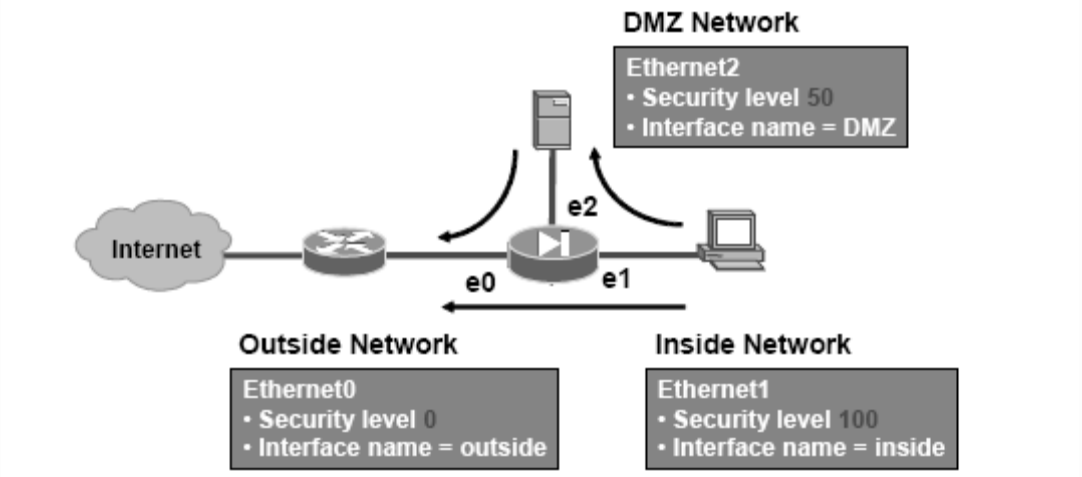
5.5.1 Αλγόριθμος ασφάλειας

Ο αλγόριθμος ασφάλειας είναι μια αναλυτική (stateful) προσέγγιση στην ασφάλεια. Κάθε εισερχόμενο πακέτο (το πακέτο που προέρχεται από ένα σύστημα σε ένα λιγότερο προστατευμένο δίκτυο και προορίζεται για ένα σύστημα σε ένα περισσότερο προστατευμένο δίκτυο) ελέγχεται σε σχέση με τις πληροφορίες κατάστασης σύνδεσης. Ο έλεγχος υλοποιείται με τις παρακάτω εργασίες:

- Εφαρμόζεται αναλυτικός έλεγχος σύνδεσης μέσω της συσκευής ασφάλειας.
- Επιτρέπονται η εξερχόμενες συνδέσεις μιας κατεύθυνσης (one-way) μετά από ένα ελάχιστο αριθμό αλλαγών διαμόρφωσης.
- Γίνετε παρακολούθηση των πακέτων που επιστρέφουν για να εξασφαλιστεί η εγκυρότητα τους.
- Δημιουργεί συνθήκες τυχαιότητας (randomizes) αλλάζοντας τον πρώτο αριθμό ακολουθίας TCP ώστε να ελαχιστοποιηθεί ο κίνδυνος επίθεσης.

5.5.2 Επίπεδα ασφάλειας

Το επίπεδο ασφάλειας υποδεικνύει εάν μια διεπαφή θα θεωρηθεί έμπιστη και προστατευμένη ή μη έμπιστη (untrusted) και λιγότερο προστατευμένη σχετικά με μια άλλη διεπαφή. Μια διεπαφή θεωρείται έμπιστη σε σχέση με μια άλλη μονό εάν το επίπεδο ασφάλειάς είναι πιο υψηλό από το επίπεδο ασφάλειας της άλλης διεπαφής. Θεωρείται μη έμπιστη εάν το επίπεδο ασφάλειάς είναι χαμηλότερο από το επίπεδο ασφάλειας της άλλης διεπαφής. Ο βασικός κανόνας για τα επίπεδα ασφάλειας αναφέρει ότι μια διεπαφή με υψηλότερο επίπεδο ασφάλειας μπορεί να έχει πρόσβαση σε μια διεπαφή με χαμηλότερο επίπεδο ασφάλειας. Τα επίπεδα ασφάλειας, κυμαίνονται από 0 έως 100, με την τιμή μηδέν για την εξωτερική διεπαφή και 100 στην εσωτερική. Ένα παράδειγμα με τρία επίπεδα ασφάλειας απεικονίζεται στο σχήμα 5-2.



Σχήμα 5-2 : Παράδειγμα επιπέδων ασφάλειας

Επίπεδο ασφάλειας 100: Είναι το πιο υψηλό επίπεδο ασφάλειας για την εσωτερική διεπαφή της συσκευής ασφάλειας. Αποτελεί προεπιλεγμένη ρύθμιση και δεν μπορεί να αλλάξει. Επειδή το πιο έμπιστο επίπεδο ασφάλειας διεπαφών είναι 100, το εταιρικό δίκτυό πρέπει να εγκατασταθεί πίσω από αυτή τη διεπαφή, έτσι ώστε κανένας άλλος να μην μπορεί να έχει πρόσβαση στο εσωτερικό δίκτυο, εκτός αν δίνεται συγκεκριμένη άδεια. Κάθε συσκευή πίσω από αυτήν την διεπαφή μπορεί να έχει πρόσβαση έξω από το εταιρικό δίκτυο.

Επίπεδο ασφάλειας 0: Αποτελεί το χαμηλότερο επίπεδο ασφάλειας για την εξωτερική διεπαφή της συσκευής ασφάλειας. Είναι προεπιλεγμένη ρύθμιση και δεν μπορεί να αλλάξει. Επειδή το λιγότερο έμπιστο επίπεδο ασφάλειας διεπαφών είναι 0, πρέπει να τοποθετηθεί το λιγότερο έμπιστο δίκτυό πίσω από αυτήν την διεπαφή, έτσι ώστε να μην έχει πρόσβαση σε άλλες διεπαφές εκτός και αν δίνεται συγκεκριμένη άδεια. Αυτή η διεπαφή χρησιμοποιείται συνήθως για τη σύνδεση με το διαδίκτυό.

Επίπεδα ασφάλειας 1 έως 99: Είναι τα υπόλοιπα επίπεδα ασφάλειας και μπορούν να χρησιμοποιηθούν από τις περιμετρικές διεπαφές που συνδέονται με τη συσκευή ασφάλειας. Τα επίπεδα ασφάλειας θα πρέπει να βασίζονται στον τύπο πρόσβασης που θα πρέπει να έχει το κάθε σύστημα.

5.6 Βασική διαμόρφωση

Αυτή η ενότητα περιέχει τις βασικές εντολές που καθιστούν λειτουργική μια συσκευή ασφάλειας. Παρακάτω περιγράφονται μερικές από τις αρχικές εντολές διαμόρφωσης.

Ανάθεση ονόματος στη συσκευή ασφάλειας: Στο παράδειγμα 5-11 η εντολή *hostname* αλλάζει το όνομα της συσκευής από pixfirewall σε fw1 .

Παράδειγμα 5-11 : Ανάθεση ονόματος
pixfirewall(config)# hostname fw1 fw1(config)#

Εντολή *interface*: Η εντολή *interface* προσδιορίζει μια διεπαφή και τη θέση της (slot location) στη συσκευή ασφάλειας. Μετά από την εισαγωγή της εντολής, όπως και στο παράδειγμα 5-12, η υπαγόρευση στο CLI αλλάζει στο επίπεδο υποεντολών (subcommand) διαμόρφωσης διεπαφών. Σε αυτή την κατάσταση, μπορούμε να διαμορφώσουμε την αμφίδρομη λειτουργία και ταχύτητα (hardware speed and duplex), να ορίσουμε το όνομα της διεπαφής, το επίπεδο ασφάλειας, την διεύθυνση IP και να πολλές άλλες ρυθμίσεις. Μια διεπαφή για

να μπορέσει να διαχειριστεί κυκλοφορία, θα πρέπει πρώτα να διαμορφωθούν οι παρακάτω υποεντολές: *nameif, ip address, security-level, no shutdown.*

Παράδειγμα 5-12 : Εντολή *interface*
fw1(config)# interface ethernet0 fw1(config-if)#

Ρύθμιση ονόματος διεπαφής: Η υποεντολή *nameif* ορίζει ένα όνομα σε κάθε διεπαφή της συσκευής ασφάλειας. Οι πρώτες δύο διεπαφές έχουν τα ονόματα προεπιλογής *inside* και *outside*. Στο παράδειγμα 5-13, στη διεπαφή Ethernet2 ορίζεται το όνομα *dmz*.

Παράδειγμα 5-13 : Ρύθμιση ονόματος σε μια διεπαφή
fw1(config-if)# nameif outside

Ρύθμιση της διεύθυνσης IP: Κάθε διεπαφή στη συσκευή ασφάλειας μπορεί να διαμορφωθεί με μια διεύθυνση IP. Η υποεντολή *ip address* ορίζει την αντίστοιχη διεύθυνση.

Παράδειγμα 5-14 : Ρύθμιση της διεύθυνσης IP
fw1(config-if)# ip address 192.168.1.2 255.255.255.0

Ρύθμιση της διεύθυνσης IP μέσω DHCP: Αντί να διαμορφώσουμε μια διεύθυνση IP στη διεπαφή, μπορούμε να ενεργοποιήσουμε στη συσκευή ασφάλειας το χαρακτηριστικό πελάτη DHCP για να ανακτήσει δυναμικά μια διεύθυνση IP από ένα διακομιστή DHCP (Dynamic Host Configuration Protocol).

Παράδειγμα 5-15 : Ρύθμιση της διεύθυνσης IP μέσω DHCP
fw1(config-if)# ip address dhcp

Ρύθμιση επίπεδων ασφάλειάς: Η υποεντολή *security-level* διευκρινίζει το επίπεδο ασφάλειας σε μια διεπαφή (εκτός από τις εσωτερικές και εξωτερικές διεπαφές, οι οποίες έχουν συγκεκριμένα επίπεδα ασφάλειας εξ ορισμού).

Παράδειγμα 5-16 : Ρύθμιση επιπέδου ασφάλειας
fw1# configure terminal fw1(config)# interface ethernet0 fw1(config-if)# security-level 0

Ρύθμιση ταχύτητας και αμφίδρομης λειτουργίας: Στην αρχική διαμόρφωση η ταχύτητα υλικού είναι στην αυτόματη ρύθμιση. Για να ορίσουμε την ταχύτητα μιας διεπαφής Ethernet (RJ-45), χρησιμοποιούμε την υποεντολή *speed,* ενώ για την αμφίδρομη λειτουργία την υποεντολή *duplex*. Για να επαναφέρουμε την προεπιλεγμένη ρύθμιση, χρησιμοποιούμε τη μορφή *no* της εντολής.

Παράδειγμα 5-17 : Ρύθμιση ταχύτητας και αμφίδρομης λειτουργίας
fw1(config)# interface ethernet0 fw1(config-if)# speed 100 fw1(config-if)# duplex full

Ρύθμιση διεπαφής διαχείρισης: Για να διαμορφώσουμε μια διεπαφή ώστε να δέχεται μόνο κυκλοφορία διαχείρισης (management traffic), χρησιμοποιούμε την υποεντολή the *management-only*.

Παράδειγμα 5-18 : Ρύθμιση διεπαφής διαχείρισης
fw1(config)# interface ethernet2 fw1(config-if)# management-only

Κατάλογος χαρτογράφησης: Η χρήση της εντολής *name* επιτρέπει την διαμόρφωση ενός κατάλογου χαρτογράφησης όνομα με IP. Επιτρέπει στην ουσία τη διαμόρφωση με χρήση των ονομάτων αντί των διευθύνσεων IP.

Παράδειγμα 5-19 : Σύνδεση ονόματος με IP
fw1(config)# names fw1(config)# name 172.16.0.2 bastionhost fw1(config)# name 10.0.0.11 insidehost

5.7 Έλεγχος κατάστασης

Αυτή η ενότητα περιέχει τις βασικές εντολές *show* που απαιτούνται για των έλεγχο της κατάστασης διαμόρφωσης και υλικού των συσκευών ασφάλειας.

Παράδειγμα 5-20 : Έλεγχος διαμόρφωσης
fw1(config)# show run interface

Η εντολή *show run* συν μια παράμετρο εμφανίζει μια στατική οθόνη, ενώ η εντολή *show* σε συνδυασμό με παράμετρο εμφανίζει μια δυναμικά μεταβαλλόμενη οθόνη στατιστικών. Π.χ. η έξοδος της εντολής *show run interface* δείχνει πώς είναι διαμορφωμένες οι διεπαφές, μια στατική οθόνη, ενώ η έξοδος της εντολής *show interface* είναι μια δυναμική οθόνη με counters.

Παράδειγμα 5-21 : Έλεγχος κατάστασης
fw1(config)# show interface

Έλεγχος μνήμης: Η έξοδος της εντολής *show memory* εμφανίζει μια περίληψη της μέγιστης φυσικής μνήμης, της τρέχουσας χρησιμοποιημένης μνήμης και της τρέχουσας διαθέσιμης ελεύθερης μνήμης στο λειτουργικό σύστημα.

Παράδειγμα 5-22 : Έλεγχος μνήμης
fw1# show memory

Έλεγχος χρήσης CPU: Η έξοδος της εντολής *show cpu usage* εμφανίζει τα στατιστικά χρήσης της CPU.

Παράδειγμα 5-23 : Έλεγχος χρήσης CPU
fw1# show cpu usage

Εντολή *show version*: Εμφανίζει σαν έξοδο την έκδοση του λογισμικού , το χρόνο λειτουργίας της συσκευής από την τελευταία επανεκκίνηση, τον τύπο επεξεργαστή, τον τύπο μνήμης Flash, τους πίνακες διεπαφών, τον σειριακό αριθμό, και το κλειδί ενεργοποίησης (activation key).

Παράδειγμα 5-24 : Έλεγχος έκδοσης
fw1# show version

Εντολή *show ip address*: Επιτρέπει τον έλεγχο των διευθύνσεων IP που έχουν διαμορφωθεί στις διεπαφές δικτύων. Οι τρέχουσες διευθύνσεις IP είναι ίδιες με τις διευθύνσεις IP στην ενεργή συσκευή ασφάλειας failover. Όταν η ενεργή συσκευή ασφάλειας αποτυγχάνει, οι τρέχουσες διευθύνσεις IP γίνονται αυτές της εφεδρικής συσκευής ασφάλειας.

Παράδειγμα 5-25 : Έλεγχος ενεργών διευθύνσεων IP
fw1# show ip address

Εντολή *show interface* : Εμφανίζει σαν έξοδο τις πληροφορίες δικτυού. Είναι μια από τις πρώτες εντολές που θα πρέπει να χρησιμοποιηθούν κατά την προσπάθεια διαπίστωσης συνδεσιμότητας (connectivity). Παρακάτω παρουσιάζονται μερικές επεξηγήσεις των πληροφοριών που εμφανίζονται αφού εκτελέσουμε την εντολή:

- Ethernet: Δείχνει ότι έχει χρησιμοποιηθεί η εντολή *interface* για την διαμόρφωση της διεπαφής. Εμφανίζει εάν η διεπαφή είναι εσωτερική ή εξωτερική και εάν είναι διαθέσιμη (up) ή μη διαθέσιμη (down).
- Line protocol up: Σημαίνει ότι ένα καλώδιο λειτουργεί και είναι συνδεμένο με τη διεπαφή δικτύων.
- Line protocol down: Το καλώδιο που συνδέεται με τη διεπαφή δικτύων είναι λάθος ή δεν είναι συνδεμένο με το συνδετήρα διεπαφών.

Παράδειγμα 5-26 : Έλεγχος πληροφοριών διεπαφής
fw1# show interface interface ethernet0 "outside" is up, line protocol is up …

Εντολή *show nameif*: Εμφανίζει σαν έξοδο τα ονόματα των διεπαφών και τα αντίστοιχα επίπεδο ασφάλειας.

Παράδειγμα 5-27 : Έλεγχος ονομαστικών διεπαφών
fw1# show nameif

5.8 Ρύθμιση ώρας και υποστήριξη NTP

Σε αυτή την ενότητα παρουσιάζεται η διαμόρφωση της ώρας στη συσκευή ασφάλειας και ο συγχρονισμός του χρόνου με τις άλλες συσκευών που λειτουργούν σε ένα δίκτυο δεδομένων IP.

Εντολή *clock:* Ρυθμίζει το ρολόι της συσκευής ασφάλειας. Επιτρέπει τον καθορισμό της ώρας, του μήνα, της ημέρα και του έτους. Η συσκευή ασφάλειας παράγει μηνύματα για τα γεγονότα του συστήματος και μπορεί να καταγράψει αυτά τα μηνύματα σε έναν syslog server. Εάν θέλουμε τα μηνύματα να περιέχουν μια τιμή χρόνου time-stamp, τότε πρέπει να εισάγουμε την εντολή *logging timestamp*. Εάν χρησιμοποιηθεί κάποια δημόσια υποδομή κλειδιού (PKI) με ψηφιακά πιστοποιητικά για την επικύρωση των VPN συνδέσεων, είναι σημαντικό να εξασφαλιστεί ότι το ρολόι έχει διαμορφωθεί σωστά. Διαφορετικά, η αρχή πιστοποιητικών (CA) μπορεί να απορρίψει ή να επιτρέψει τα πιστοποιητικά βασισμένα σε ένα ανακριβές time-stamp. Μπορούμε να παρατηρήσουμε το χρόνο με την εντολή *show clock*, η οποία εμφανίζει την ώρα, τη χρονική ζώνη, την ημέρα και την πλήρη ημερομηνία. Η εντολή *clock set* μπορεί να αφαιρεθεί από την εντολή *clear configure clock* .

Παράδειγμα 5-28 : Ρύθμιση ώρας
fw1# clock set 21:01:01 jan 17 2008

Εντολή *ntp*: Συγχρονίζει τη συσκευή ασφάλειας με τον διακομιστή NTP και δίνει τη δυνατότητα για διαμόρφωση που θα απαιτεί επικύρωση πριν απο το συγχρονισμό με τον διακομιστή NTP. Όπως δείχνει και το παράδειγμα 5-29 για να ενεργοποιηθεί η επικύρωση, χρησιμοποιούνται οι εντολές *ntp* και *ntp server*.

Παράδειγμα 5-29 : Καθορισμός NTP server
fw1(config)# ntp authentication-key 1234 md5 pass123
fw1(config)# ntp trusted-key 1234
fw1(config)# ntp server 10.0.0.12 key 1234 source inside prefer
fw1(config)# ntp authenticate

5.9 Διαμόρφωση Syslog

Αυτή η ενότητα επεξηγεί την διαμόρφωση τις συσκευές ασφάλειας για να στείλει log μηνύματα σε ένα syslog server. Η συσκευή ασφάλειας παράγει μηνύματα για τα γεγονότα συστήματος, όπως οι συναγερμοί και η μείωση των πόρων. Τα syslog μηνύματα μπορούν να χρησιμοποιηθούν για να δημιουργήσουν αρχεία ημερολογίου ή να εμφανίζονται στην κονσόλα ενός syslog host. Παρακάτω παρουσιάζονται οι διαθέσιμες επιλογές αναγραφής :

- ***Console****:* Εμφανίζει στην κονσόλα τα log μηνύματα.
- ***Buffered****:* Στέλνει τα log μηνύματα σε έναν εσωτερικό απομονωτή (buffer), από τον όποιο μπορούν στη συνεχεία να τα δούμε με την εντολή *show logging.*
- ***Monitor****:* Διευκρινίζει ότι τα log μηνύματα θα εμφανίζονται στην κονσόλα των τερματικών που έχουν συνδεθεί με Telnet.
- ***Host:*** Διευκρινίζει τον log server ο όποιος θα λάβει τα μηνύματα που στέλνονται από τη συσκευή ασφάλειας.
- ***SNMP:*** Επιτρέπει την αποστολή των log μηνυμάτων ως ανακοινώσεις παγίδων SNMP (trap notifications).

Στο παράδειγμα 5-30, η συσκευή ασφάλειας διαμορφώνεται για να στείλει τα log μηνύματα στον Syslog server με IP 10.0.0.12. Τα μηνύματα που στέλνονται θα περιλαμβάνουν μηνύματα προειδοποίησης καθώς και τα μηνύματα υψηλότερης σημαντικότητας. Κάθε μήνυμα θα είναι χρόνο-σφραγισμένο και θα έχει σαν προσδιοριστικό συσκευής την λέξη fw1. Η τελευταία εντολή ενεργοποιεί την καταγραφή.

Παράδειγμα 5-30 : Διαμόρφωση για αποστολή μηνυμάτων σε Syslog Server
fw1(config)# logging host inside 10.0.1.11
fw1(config)# logging trap warnings
fw1(config)# logging timestamp
fw1(config)# logging device-id fw1
fw1(config)# logging on

Η συσκευή ασφάλειας συνδέει επίσης κάθε ταυτότητα μηνύματος (message ID) με ένα επίπεδο σημαντικότητας (severity level) που κυμαίνεται από 0 έως 7. Όσο χαμηλότερος είναι ο αριθμός, τόσο κρισιμότερο είναι το μήνυμα. Στον πίνακα 5-2 παρουσιάζονται τα επίπεδα σημαντικότητας, μαζί με τη σχετική λέξη κλειδί και μια συνοπτική περιγραφή.

Πίνακας 5-2 : Επίπεδα σημαντικότητας

Επίπεδο	*Λέξη κλειδί*	*Περιγραφή*
0	emergencies	Γεγονός που χρησιμοποιείται για να δείξει ότι το σύστημα είναι ακατάλληλο προς χρήση
1	alerts	Μήνυμα που χρησιμοποιείται για να διευκρινίσει ότι απαιτείται μια άμεση δράση.
2	critical	Μήνυμα που χρησιμοποιείται για να διευκρινίσει μια κρίσιμη κατάσταση, π.χ. επίθεση.
3	errors	Γεγονός που χρησιμοποιείται για τα μηνύματα λάθους.
4	warnings	Γεγονός που χρησιμοποιείται για να ενημερώσει για τα μηνύματα προειδοποίησης, όπως η υπέρβαση ορισμένων κατώτατων ορίων.
5	notifications	Μήνυμα που χρησιμοποιείται για να προσδιορίσει ένα κανονικό αλλά σημαντικό γεγονός.
6	informational	Γεγονός που χρησιμοποιείται για να ταξινομήσει τα ενημερωτικά μηνύματα.
7	debugging	Γεγονός που χρησιμοποιείται για να δείξει το πιο αναλυτικό επίπεδο εντοπισμού σφαλμάτων (low-level debug).

ΚΕΦΑΛΑΙΟ 6

Μεταφράσεις και συνδέσεις

6.1 Εισαγωγή

Αυτό το κεφαλαίο αναφέρεται στις μεταφράσεις και συνδέσεις των συσκευών ασφάλειας. Πρώτα, αναλύεται ο τρόπος που οι συσκευές ασφάλειας επεξεργάζονται την κυκλοφορία TCP και UDP. Στη συνεχεία μελετάται η διαμόρφωση των συσκευών ασφάλειας για να υποστηρίξουν τις δυναμικές και στατικές μεταφράσεις διευθύνσεων.

6.2 Πρωτόκολλα μεταφορών

Αυτή η ενότητα έχει σαν στόχο την κατανόηση των πρωτοκόλλων ελέγχου μεταφοράς - TCP και διαγραμμάτων δεδομένων χρηστών - UDP. Αυτό κρίνεται απαραίτητο για να καταλάβουμε και το πώς λειτουργεί η συσκευή ασφάλειας. Σε ένα δίκτυο IP, σύνοδος δικτύων ονομάζεται η συναλλαγή που πραγματοποιείται μεταξύ δύο συστημάτων πάνω από δύο πρωτόκολλα του στρώματος μεταφορών:

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

Το πρωτόκολλο TCP είναι προσανατολισμένο προς τη σύνδεση (connection-oriented). Όταν μια σύνοδος ξεκινά από έναν ασφαλέστερο σύστημα στο εσωτερικό δίκτυο, η συσκευή ασφάλειας δημιουργεί μια είσοδο στο φίλτρο κατάστασης συνόδου (session state filter). Η συσκευή ασφάλειας είναι σε θέση να εξαγάγει τις συνόδους δικτύων από τη ροή κυκλοφορίας και να ελέγχει ενεργά την ισχύ τους σε πραγματικό χρόνο. Αυτό το stateful φίλτρο διατηρεί την κατάσταση κάθε σύνδεσης και ελέγχει τις επόμενες μονάδες πρωτοκόλλου

σε σχέση με τα αναμενόμενα αποτελέσματα. Κάθε φορά που δημιουργείται μια σύνοδος TCP, η συσκευή ασφάλειας καταγράφει τη ροή κυκλοφορίας και αναζητεί μια αναγνώριση για την συσκευή με την οποία ο host προσπαθεί να ξεκινήσει επικοινωνία. Έπειτα, η συσκευή ασφάλειας επιτρέπει την κυκλοφορία μεταξύ των συστημάτων, βασισμένη στην τριπλή χειραψία (three-way handshake).

Το πρωτόκολλο UDP είναι χωρίς σύνδεση (connectionless). Σε αυτή την περίπτωση η συσκευή ασφάλειας πρέπει να λάβει άλλα μέτρα για να εξασφαλιστεί η ασφάλειά. Οι εφαρμογές που χρησιμοποιούν UDP είναι δύσκολο να προστατεύουν κατάλληλα επειδή δεν υπάρχει καμία χειραψία ή αλληλουχία (sequencing) ώστε να καθοριστεί η τρέχουσα κατάσταση μιας συναλλαγής UDP. Είναι επίσης δύσκολο να διατηρηθεί η κατάσταση μιας συνόδου επειδή δεν έχει ξεκάθαρη αρχή, κατάσταση ροής ή τέλος. Ωστόσο, η συσκευή ασφάλειας δημιουργεί μια υποδοχή σύνδεσης (connection slot) όταν στέλνεται ένα πακέτο UDP από μια ασφαλέστερη σε μια λιγότερο ασφαλή διεπαφή. Όλα τα επόμενα επιστρεφόμενα πακέτα UDP που ταιριάζουν με την υποδοχή σύνδεσης διαβιβάζονται στο εσωτερικό δίκτυο.

6.3 Μετάφραση διευθύνσεων δικτύων

Σε αυτή την ενότητα περιγράφεται η διαδικασία της μετάφρασης στις συσκευές ασφάλειας. Υπάρχουν δύο τύποι εσωτερικών μεταφράσεων : δυναμική και στατική.

Σχήμα 6-1 : Μετάφραση διευθύνσεων

Η Μετάφραση Διευθύνσεων Δικτύων (Network Address Translation - NAT) δημιουργήθηκε για την επίλυση αρκετών προβλημάτων που εμφανίστηκαν με την επέκταση του Διαδικτύου:

- Για να δώσει λύση στο πρόβλημα του περιορισμένου αριθμού διευθύνσεων.
- Για να χρησιμοποιήσει εσωτερικά τις διευθύνσεις RFC 1918.
- Για να συντηρήσει το εσωτερικό σχέδιο διευθύνσεων
- Για να αυξήσει την ασφάλεια με την απόκρυψη της εσωτερικής τοπολογίας.

Στον σχήμα 6-1, το ιδιωτικό δίκτυο χρησιμοποιεί τις ιδιωτικές διευθύνσεις IP που ανήκουν στο δίκτυο 10.0.0.0/24. Για να μπορέσει ένα πακέτο να σταλεί στο διαδίκτυο, πρέπει πρώτα να μεταφραστεί σε μια δημόσια διεύθυνση που μπορεί να δρομολογηθεί (routable). Σε αυτό το παράδειγμα, η συσκευή ασφάλειας μεταφράζει την IP διεύθυνση 10.0.0.11 στην IP routable διεύθυνση 192.168.6.9

Πρόσβαση μέσω της συσκευής ασφάλειας:

Όταν διαμορφώνουμε τις διεπαφές, θα πρέπει να έχουμε υπόψη ότι το επίπεδο ασφάλειας υποδεικνύει εάν μια διεπαφή είναι εσωτερική (έμπιστη) ή εξωτερική (μη έμπιστη) σχετικά με μια άλλη διεπαφή. Συμφώνα με το βασικό κανόνα για τα επίπεδα ασφάλειας μια διεπαφή με υψηλότερο επίπεδο ασφάλειας μπορεί να έχει πρόσβαση σε μια διεπαφή με χαμηλότερο επίπεδο ασφάλειας. Οι εντολές *nat* και *global* λειτουργούν μαζί για να επιτρέψουν στο δίκτυό να χρησιμοποιήσει οποιοδήποτε σχέδιο IP. Επιπλέον οι δυο εντολές χρησιμοποιούνται για να παραμείνουν οι διευθύνσεις αυτές κρυμμένες από το εξωτερικό δίκτυο, προσφέροντας με αυτό το τρόπο ένα προσθετό επίπεδο ασφάλειας στο εσωτερικό δίκτυο. Μια διεπαφή με ένα χαμηλότερο επίπεδο ασφάλειας δεν μπορεί να έχει πρόσβαση σε μια διεπαφή με ένα υψηλότερο επίπεδο ασφάλειας, εκτός αν συγκεκριμένα της επιτραπεί από την εφαρμογή των εντολών *static* και *access list*.

6.3.1 Εσωτερική μετάφραση διευθύνσεων

Η συσκευή ασφάλειας υποστηρίζει δύο τύπους μεταφράσεων διευθύνσεων:

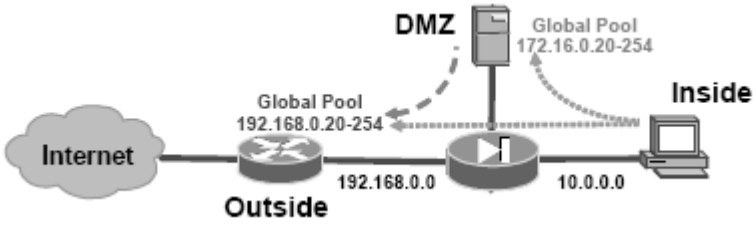
- **Στατική μετάφραση:** Παρέχει μόνιμη, μια προς μια, χαρτογράφηση μεταξύ μιας διεύθυνσης IP σε μια ασφαλέστερη διεπαφή και μιας διεύθυνσης IP σε μια λιγότερο ασφαλή διεπαφή. Αυτό επιτρέπει σε ένα εσωτερικό σύστημα την πρόσβαση σε ένα λιγότερο ασφαλή σύστημα, χωρίς έκθεση της πραγματικής διεύθυνσης IP. Παραδείγματα στατικής μετάφρασης είναι το στατικό και το ταυτοποιημένο (identity) NAT.

- **Δυναμική μετάφραση:** Μεταφράζει τις διευθύνσεις στις ασφαλέστερες διεπαφές, σε μια σειρά ή μια ομάδα διευθύνσεων IP, σε μια λιγότερο ασφαλή διεπαφή. Αυτό επιτρέπει στους εσωτερικούς χρήστες να μοιράζονται τις καταχωρημένες (registered) διευθύνσεις IP και να αποκρύψουν τις εσωτερικές διευθύνσεις από το να γίνουν ορατές.

Οι δυναμικές εσωτερικές μεταφράσεις χρησιμοποιούνται για τα τοπικά συστήματα και τις εξερχόμενες συνδέσεις τους και κρύβουν τη διεύθυνση IP από το διαδίκτυο. Στις δυναμικές μεταφράσεις, πρέπει πρώτα να καθορίσουμε ποια συστήματα είναι επιλέξιμα για μετάφραση με την εντολή *nat* και στη συνεχεία να καθορίσουμε το εύρος διευθύνσεων με τη εντολή *global*. Το εύρος της κατανομής διευθύνσεων επιλέγεται στην εξερχόμενη διεπαφή βασισμένη στο προσδιοριστικό NAT (NAT identifier- NAT ID) που επιλέγεται με την εντολή *nat*. Στο παράδειγμα 6-1, όλα τα συστήματα στο εσωτερικό δίκτυο είναι επιλέξιμα για μετάφραση. Το εύρος κατανομής των διευθύνσεων ορίζεται από την εντολή *global* και είναι από 192.168.0.20 μέχρι 192.168.0.254, επιτρέποντας μέχρι 235 προσωπικές διευθύνσεις IP.

Παράδειγμα 6-1 : Δυναμική μετάφραση
fw1(config)# nat (inside) 1 10.0.0.0 255.255.255.0 fw1(config)# global (outside) 1 192.168.0.20-192.168.0.254 netmask 255.255.255.0

6.3.2 Παράδειγμα NAT με τρεις διεπαφές



Σχήμα 6-2 : Δίκτυο με τρεις διεπαφές και NAT

Στο παράδειγμα 6-2, η πρώτη εντολή *nat* επιτρέπει στα συστήματα που είναι τοποθετημένα στην εσωτερική διεπαφή να ξεκινούν συνδέσεις με συστήματα σε διεπαφές με χαμηλότερα επίπεδα ασφάλειας. Στη περίπτωση μας, περιλαμβάνει τους hosts στην εξωτερική διεπαφή και τους hosts στην αποστρατικοποιημένη ζώνη (DMZ). Η δεύτερη εντολή *nat* επιτρέπει στους hosts στην DMZ να ξεκινούν συνδέσεις με τους hosts στις διεπαφές με χαμηλότερα επίπεδα ασφάλειας. Σε αυτήν την περίπτωση, περιλαμβάνει μόνο την εξωτερική διεπαφή.

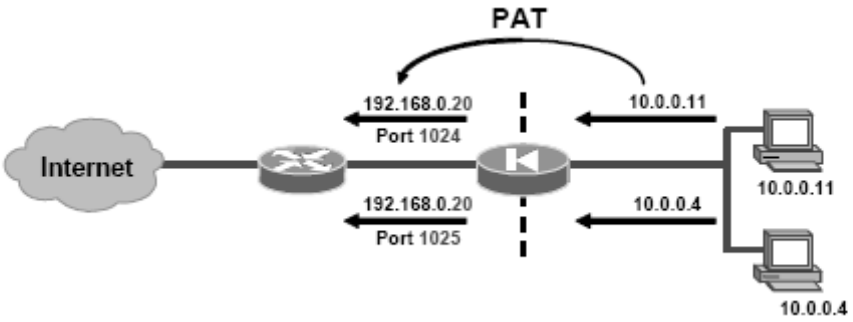
Παράδειγμα 6-2 : Δίκτυο με τρεις διεπαφές και NAT
fw1(config)# nat (inside) 1 10.0.0.0 255.255.255.0 fw1(config)# nat (dmz) 1 172.16.0.0 255.255.255.0 fw1(config)# global (outside) 1 192.168.0.20-192.168.0.254 netmask 255.255.255.0 fw1(config)# global (dmz) 1 172.16.0.20-172.16.0.254 netmask 255.255.255.0

Επειδή το εύρος κατανομής και στις δυο περιπτώσεις των εντολών *nat (inside)* χρησιμοποιεί το ίδιο NAT ID 1, οι διευθύνσεις για τους hosts στο δίκτυο 10.0.0.0 μπορούν να μεταφραστούν στο εύρος 192.168.0.20-192.168.0.254 αλλά και στο 172.16.0.20-172.16.0.254. Επομένως, όταν οι χρήστες στην εσωτερική διεπαφή θα θέλουν να έχουν πρόσβαση στους hosts στην DMZ, η εντολή *global (dmz)* αναγκάζει τις διευθύνσεις προέλευσής να μεταφραστούν στις διευθύνσεις 172.16.0.20 έως 172.16.0.254.

Όταν θα ξεκινήσουν σύνδεση σε κάποιο εξωτερικό δίκτυο, η εντολή *global (outside)* αναγκάζει τις διευθύνσεις προέλευσής να μεταφραστούν στις διευθύνσεις 192.168.0.20 έως 192.168.0.254. Στη περίπτωση που οι χρήστες στη DMZ θα θέλουν να έχουν πρόσβαση στους εξωτερικούς hosts, μέσω της εντολής *global (outside)* οι διευθύνσεις προέλευσής θα μεταφραστούν στις διευθύνσεις 192.168.0.20 έως 192.168.0.254.

6.4 Μετάφραση διευθύνσεων θύρας

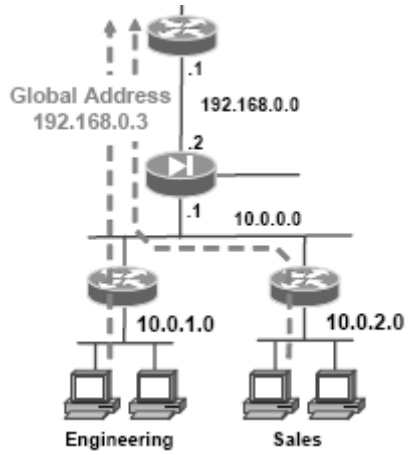
Αυτή η ενότητα περιγράφει τον τρόπο διαμόρφωσης μιας συσκευής ασφάλειας για να χρησιμοποίει μετάφραση διευθύνσεων θύρας (port address translation - PAT). Στον σχήμα 6-3, οι διευθύνσεις IP των δύο συστημάτων στο εσωτερικό δίκτυο είναι μεταφρασμένες σε μια διεύθυνση PAT, την IP 192.168.0.20 και της θύρες πηγής 1024 και 1025.



Σχήμα 6-3 : Μετάφραση διευθύνσεων θύρας

- Η μετάφραση διευθύνσεων θύρας είναι ένας συνδυασμός μιας διεύθυνσης IP και ενός αριθμού θύρας πηγής.
- Διαφορετικές συνδέσεις μπορούν να κάνουν χρήση μονό μιας σφαιρικής διεύθυνσης IP (global IP address).
- Οι συνδέσεις παραμένουν ευδιάκριτες με την χρήση των διαφορετικών αριθμών θύρας.

6.4.1 Παράδειγμα PAT

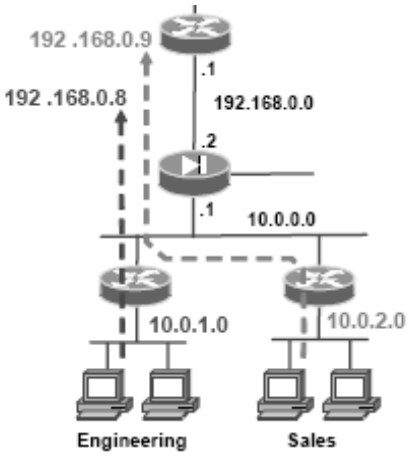


Σχήμα 6-4 : PAT

Οι εξωτερικές διευθύνσεις IP καταχωρούνται συμφώνα με τα αντίστοιχα InterNIC. Οι διευθύνσεις προέλευσης στο δίκτυο 10.0.0.0 για εξερχόμενη πρόσβαση μεταφράζονται σε 192.168.0.3. Μια ενιαία διεύθυνση IP (192.168.0.3) ορίζεται σαν εύρος κατανομής. Η θύρα πηγής αλλάζει δυναμικά σε ένα μοναδικό αριθμό που είναι μεγαλύτερος από 1023.

Παράδειγμα 6-4 : PAT
fw1(config)# route (outside) 0.0.0.0 0.0.0.0 192.168.0.1
fw1(config)# nat (inside) 1 10.0.0.0 255.255.0.0
fw1(config)# global (outside) 1 192.168.0.3 netmask 255.255. 255.255

6.4.2 Παράδειγμα χαρτογράφησης υποδικτύων και PAT

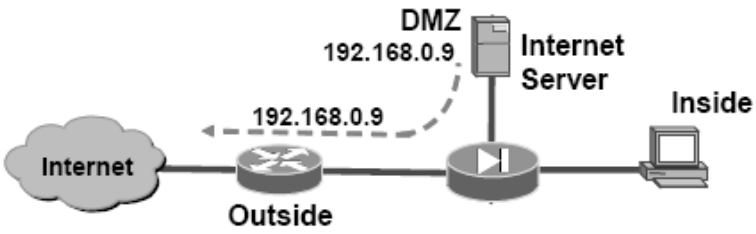


Σχήμα 6-5 : Δυο υποδίκτυα και PAT

Κάθε εσωτερικό υποδίκτυο χαρτογραφείται σε μια διαφορετική διεύθυνση PAT. Οι διευθύνσεις προέλευσης των hosts στο δίκτυο 10.0.1.0 μεταφράζονται σε 192.168.0.8 για την εξερχόμενη πρόσβαση. Οι διευθύνσεις προέλευσης των hosts στο δίκτυο 10.0.2.0 μεταφράζονται σε 192.168.0.9 για την εξερχόμενη πρόσβαση. Η θύρα πηγής αλλάζει δυναμικά σε ένα μοναδικό αριθμό που είναι μεγαλύτερος από 1023.

Παράδειγμα 6-5 : Δυο υποδίκτυα και PAT
fw1# conf t fw1(config)# nat (inside) 1 10.0.1.0 255.255.255.0 fw1(config)# nat (inside) 2 10.0.2.0 255.255.255.0 fw1(config)# global (outside) 1 192.168.0.8 netmask 255.255.255.255 fw1(config)# global (outside) 2 192.168.0.9 netmask 255.255.255.255

6.4.3 Ταυτοποιημένο NAT



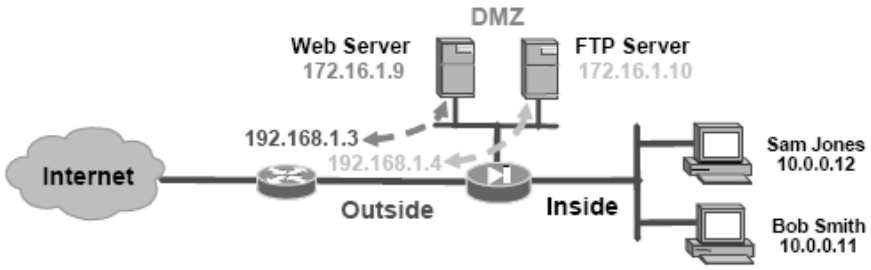
Σχήμα 6-6 : Ταυτοποιημένο NAT

Με ενεργοποιημένο τον έλεγχο NAT, όλα τα πακέτα που διαπερνούν τη συσκευή ασφάλειας χρειάζονται έναν κανόνα μεταφράσεων. Η εντολή *nat 0*, γνωστή ως identity NAT, επιτρέπει την διαφανή χαρτογράφηση των διευθύνσεων IP έτσι ώστε οι εσωτερικές διευθύνσεις IP να είναι ορατές στο εξωτερικό δίκτυο χωρίς μετάφραση διευθύνσεων. Στην εικόνα 6-6, η διεύθυνση 192.168.0.9 δεν είναι μεταφρασμένη. Όταν εκτελούμε την εντολή *nat (DMZ) 0 192.168.0.9 255.255.255.255*, η συσκευή ασφάλειας εμφανίζει ένα μήνυμα που ενημερώνει ότι το NAT 0 192.168.0.9 δεν θα μεταφραστεί. Είναι σημαντικό να σημειωθεί ότι το NAT 0 επιτρέπει στη διεύθυνση του Internet Server να είναι ορατή στην εξωτερική διεπαφή.

Παράδειγμα 6-6 : Ταυτοποιημένο NAT
fw1# conf t fw1(config)# nat (dmz) 0 192.168.0.9 255.255.255.255

6.5 Στατικό NAT

Σε αυτή την ενότητα περιγράφεται η διαμόρφωση της συσκευής ασφάλειας για μόνιμη χαρτογράφηση μεταξύ δύο διευθύνσεων IP.



Σχήμα 6-7 : Στατικό NAT

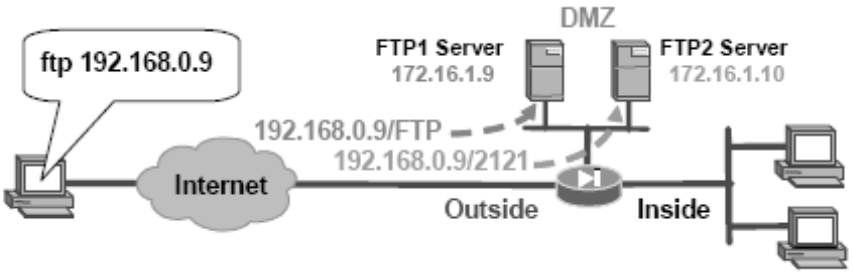
Το στατικό NAT δημιουργεί μια σταθερή μετάφραση μεταξύ των διευθύνσεων. Με το δυναμικού NAT και PAT, κάθε φορά που ένας τελικός χρήστης προσπαθεί να δημιουργήσει μια εξωτερική σύνδεση, θα μπορούσε να του δοθεί μια διαφορετική διεύθυνση. Η εντολή *static* χρησιμοποιείτε για τις εξερχόμενες συνδέσεις ώστε να εξασφαλιστεί ότι τα πακέτα από ένα εσωτερικό σύστημα χαρτογραφούνται πάντα σε μια συγκεκριμένη διεύθυνση IP (για παράδειγμα, εσωτερικό DNS ή Simple Mail Transfer Protocol host).

Παράδειγμα 6-7 : Στατικό NAT
fw1(config)# static (dmz,outside) 192.168.1.3 172.16.1.9 netmask 255.255.255.255
fw1(config)# static (dmz,outside) 192.168.1.4 172.16.1.10 netmask 255.255.255.255

Στο παράδειγμα της εικόνας 6-7, η μετάφραση εκτελείται μεταξύ της εξωτερικής και της DMZ επαφής. Η διεπαφή DMZ είναι η πραγματική, ενώ η εξωτερική διεπαφή είναι η συνδεδεμένη διεπαφή. Ο web server στη DMZ με διεύθυνση IP 172.16.1.9 μεταφράζεται σε 192.168.1.3. Η διεύθυνση IP 172.16.1.9 είναι η πραγματική διεύθυνση και 192.168.1.3 είναι ή μεταφρασμένη διεύθυνση IP.

6.6 Στατικό PAT και επαναπροσανατολισμός θυρών

Η συσκευή ασφάλειας παρέχει δυνατότητες PAT. Αυτό επιτρέπει στους εξωτερικούς χρήστες να συνδέονται σε μια συγκεκριμένη θύρα και διεύθυνση IP. Η συσκευή ασφάλειας επαναπροσανατολίζει την κυκλοφορία στον κατάλληλο εσωτερικό διακομιστή και την αντίστοιχη θύρα. Αυτή η ικανότητα μπορεί να χρησιμοποιηθεί για να στείλει τις εισερχόμενες υπηρεσίες TCP ή UDP σε διαφορετικούς εσωτερικούς υπολογιστές μέσω μιας ενιαίας σφαιρικής διεύθυνσης. Επίσης μπορεί να γίνει και μετάφραση μιας γνώστης θύρας σε μια λιγότερο γνωστή ή αντίστροφα.



Σχήμα 6-8 : Επαναπροσανατολισμός θυρών

Στο παράδειγμα της εικόνας 6-8, ένας εξωτερικός χρήστης κατευθύνει ένα αίτημα FTP στη διεύθυνση 192.168.0.9. Η συσκευή ασφάλειας επαναπροσανατολίζει το αίτημα στη DMZ, στο διακομιστή FTP με διεύθυνση IP 172.16.1.9. Για να έχει πρόσβαση στο δεύτερο διακομιστή FTP, ο εξωτερικός χρήστης κατευθύνει ένα αίτημα FTP στη διεύθυνση 192.168.0.9 και θύρα 2121. Η συσκευή ασφάλειας επαναπροσανατολίζει το αίτημα στο δεύτερο διακομιστή FTP με διεύθυνση IP 172.16.1.10.

Παράδειγμα 6-8 : Επαναπροσανατολισμός θυρών
fw1(config)# static (dmz,outside) tcp 192.168.0.9 ftp 172.16.1.9 ftp netmask 255.255.255.255 fw1(config)# static (dmz,outside) tcp 192.168.0.9 2121 172.16.1.10 ftp netmask 255.255.255.255

6.7 Όρια παρεμπόδισης και σύνδεσης TCP

Αυτή η ενότητα περιγράφει τα όρια παρεμπόδισης (intercept) και τις εμβρυικές συνδέσεις TCP και UDP. Μπορούμε να θέσουμε τα παρακάτω όρια σύνδεσης : *Emb_lin:* Μέγιστος αριθμός εμβρυικών συνδέσεων ανά υπολογιστή. Μια εμβρυική σύνδεση είναι ένα αίτημα σύνδεσης που δεν έχει ολοκληρώσει μια τριπλή χειραψία TCP μεταξύ της πηγής και του προορισμού. Για να προστατεύσουμε τα εσωτερικούς συστήματα από επιθέσεις DoS, περιορίζουμε τον αριθμό εμβρυικών συνδέσεων που επιτρέπονται στον διακομιστή. Έτσι, θέτουμε το εμβρυικό όριο συνδέσεων, ή το κατώτατο όριο, σε έναν αριθμό διαφορετικό από το μηδέν. Η τιμή μηδέν θέτει εκτός λειτουργίας την εμβρυικής προστασία συνδέσεων. Το εμβρυικό κατώτατο όριο συνδέσεων είναι διαμορφώσιμο χρησιμοποιώντας είτε τη *static* είτε τη *nat* εντολή. Στο παράδειγμα 6-9, και οι δυο εντολές ορίζουν το εμβρυικό όριο συνδέσεων σε 25.

Παράδειγμα 6-9 :Όριο εμβρυϊκών συνδέσεων
fw1(config)# nat (inside) 1 0 0 0 25 fw1(config)# static (inside,outside) 192.168.0.11 172.16.0.2 0 25

TCP_max_conns: Μέγιστος αριθμός ταυτόχρονων συνδέσεων TCP που μπορεί να χρησιμοποιήσει κάθε υπολογιστής. Οι αδρανείς συνδέσεις τερματίζονται μετά από τον προκαθορισμένο χρόνο της εντολής *timeout conn*. *Udp_max_conns*: Μέγιστος αριθμός ταυτόχρονων συνδέσεων UDP για κάθε υπολογιστή. Οι αδρανείς συνδέσεις τερματίζονται μετά από τον καθορισμένο χρόνο της εντολής *timeout conn*. Η προεπιλογή είναι μια ώρα. Στις εντολές *nat* και *static*, μπορούμε να ορίσουμε το μέγιστο αριθμό ταυτόχρονων συνδέσεων UDP με τη χρησιμοποίηση της λέξης κλειδιού *udp*. Στο παράδειγμα 6-10, η στατική σύνδεση μεταξύ 192.168.0.11 και 172.16.0.2 περιορίζεται σε ένα μέγιστο 100 συνδέσεων UDP.

Παράδειγμα 6-10 : Όριο UDP συνδέσεων
fw1(config)# nat (inside) 1 0.0.0.0 0.0.0.0 200 25 fw1(config)# static (inside,outside) 192.168.0.11 172.16.0.2 0 0 udp 100

6.8 Έλεγχος σύνδεσης και μετάφρασης

Σε αυτή την ενότητα περιγράφεται η διαφορά μεταξύ σύνδεσης και μετάφρασης και πώς αυτό μπορεί να γίνει ο αντίστοιχος έλεγχος σε μια συσκευή ασφάλειας. Οι μεταφράσεις λειτουργούν στο στρώμα IP. Για τις NAT μεταφράσεις, είναι η σύνδεση με μια πραγματική διεύθυνση IP. Για τις PAT μεταφράσεις, είναι η σύνδεση μιας διεύθυνσης και θύρας στην πραγματική διεύθυνση και πραγματικό αριθμό θύρας. Οι συνδέσεις λειτουργούν στο στρώμα μεταφοράς TCP. Οι συνδέσεις TCP πραγματοποιούνται από έναν υπολογιστή και αριθμό θύρας σε ένα άλλο υπολογιστή και αριθμό θύρας. Οι συνδέσεις είναι υποσύνολα των μεταφράσεων. Μπορεί να υπάρχουν πολλές ανοικτές συνδέσεις που χρησιμοποιούν μόνο μια μετάφραση διεύθυνσης.

Εντολή show conn: Εμφανίζει τον αριθμό των ενεργών TCP συνδέσεων και ένα σύνολο πληροφοριών. Στο παράδειγμα 6-11 υπάρχουν δύο συνδέσεις μεταξύ του υπολογιστή 10.0.0.11 και του διακομιστή ιστού 192.168.10.11. Οι συνδέσεις απευθύνονται στη θύρα TCP 80 στο διακομιστή ιστού, ενώ οι απαντήσεις απευθύνονται στον υπολογιστή 10.0.0.11 και τις θύρες 2824 2823. Στον παράδειγμα οι δύο συνδέσεις έχουν μια τιμή σημαιών UIO. Αυτό σημαίνει ότι οι σύνδεση είναι ενεργή (up) με εισερχόμενα (inbound) και εξερχόμενα (outbound) δεδομένα.

Παράδειγμα 6-11 : Έλεγχος ενεργών συνδέσεων
fw1# show conn
2 in use, 9 most used
TCP out 192.168.10.11:80 in 10.0.0.11:2824 idle 0:00:03 bytes 2320 flags UIO
TCP out 192.168.10.11:80 in 10.0.0.11:2823 idle 0:00:03 bytes 3236 flags UIO

Εντολή show local-host: Εμφανίζει τις καταστάσεις συνδέσεων των τοπικών υπολογιστών. Για κάθε υπολογιστή που διαβιβάζει κυκλοφορία μέσω της συσκευή ασφάλειας δημιουργείται ένα local host. Επιπλέον, η εντολή εμφανίζει τις υποδοχές μεταφράσεων και συνδέσεων για τους τοπικούς υπολογιστές και επιδεικνύει τις οριακές τιμές σύνδεσης.

Παράδειγμα 6-12 : Έλεγχος κατάστασης σύνδεσης
fw1# show local-host Interface inside: 0 active, 0 maximum active, 0 denied Interface outside: 1 active, 2 maximum active, 0 denied

Εντολή show xlate: Επιτρέπει να παρουσιάσουμε ή να καθαρίσουμε το περιεχόμενο των υποδοχών μετάφρασης. Η εντολή *clear xlate* θα πρέπει να χρησιμοποιηθεί μετά από αλλαγές σε λίστες έλεγχου πρόσβασης, δρομολόγηση ή τις στατικές εντολές. Στο παράδειγμα, ο υπολογιστής 10.0.0.11 μεταφράζεται από τη συσκευή ασφάλειας σε μια σφαιρική διεύθυνση 192.168.0.20.

Παράδειγμα 6-13 : Έλεγχος μεταφράσεων
fw1#show xlate 1 in use, 2 most used Global 192.168.0.20 Local 10.0.0.11

6.9 Κανόνες και φιλοσοφία μετάφρασης διευθύνσεων

Οι κανόνες των μεταφράσεων διαμορφώνονται μεταξύ των διεπαφών. Με ενεργώ έλεγχο NAT, ένα πακέτο δεν μπορεί να περάσει τη συσκευή ασφάλειας εάν δεν ταιριάζει με μια υποδοχή μετάφρασης στον πίνακα μεταφράσεων, εκτός και αν ανήκει στην κατηγορία NAT 0. Εάν δεν υπάρχει καμία υποδοχή μετάφρασης, η συσκευή ασφάλειας θα προσπαθήσει να δημιουργήσει από τους κανόνες μεταφράσεών. Στην περίπτωση που δεν βρεθεί καμία αντιστοιχία υποδοχή μετάφρασης, το πακέτο απορρίπτεται. Όταν να πακέτο φτάνει σε μια εσωτερική διεπαφή η συσκευή ασφάλειας συμβουλεύεται πρώτα τους κανόνες πρόσβασης. Λαμβάνει μια απόφαση δρομολόγησης προκειμένου να καθοριστεί η εξερχόμενη διεπαφή. Η διεύθυνση προέλευσης ελέγχεται σε σχέση με τις τοπικές διευθύνσεις στον πίνακα μεταφράσεων. Εάν υπάρχει αντίστοιχη εγγραφή, η διεύθυνση προέλευσης μεταφράζεται σύμφωνα με την υποδοχή μετάφρασης, διαφορετικά η συσκευή ασφάλειας θα αναζητήσει μια αντιστοιχία στην τοπική διεύθυνση.

ΚΕΦΑΛΑΙΟ 7
Λίστες ελέγχου πρόσβασης

7.1 Εισαγωγή

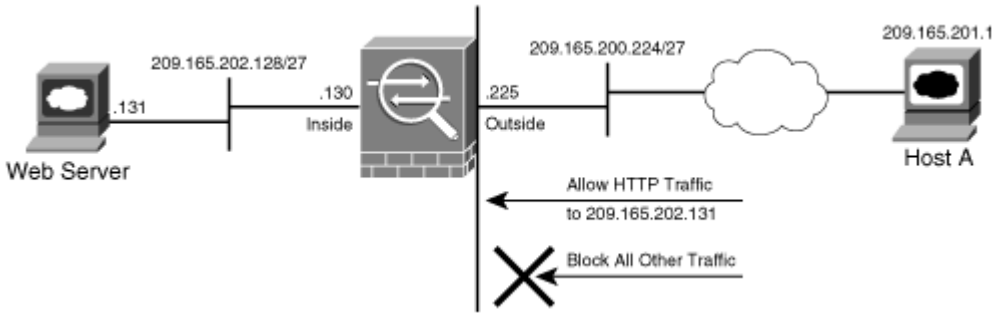
Αυτό το κεφαλαίο αναλύει τον τρόπο που οι συσκευές ασφάλειας χρησιμοποιούν τις λίστες ελέγχου πρόσβασης (access control lists - ACL) για τον έλεγχο της κυκλοφορίας. Παρουσιάζεται η θεωρία και ο τρόπος λειτουργίας των ACL μαζί με λεπτομερή παραδείγματα ειδικών περιπτώσεων ACL.

7.2 ACL

Η συσκευή ασφάλειας μπορεί να προστατεύσει το εσωτερικό δίκτυο, τις DMZ και το εξωτερικό δίκτυο επιθεωρώντας όλη την κυκλοφορία που τη διαπερνά. Μπορούμε να διευκρινίσουμε τις πολιτικές και τους κανόνες που προσδιορίζουν ποια κυκλοφορία πρέπει να επιτραπεί, εισερχόμενη ή εξερχομένη από μια διεπαφή. Η συσκευή ασφάλειας χρησιμοποιεί τις λίστες ελέγχου πρόσβασης για να απαγόρευση την ανεπιθύμητη ή άγνωστη κυκλοφορία που προσπαθεί να εισέρθει στα εμπιστευόμενα δίκτυα. Μια ACL είναι ένας κατάλογος κανόνων ασφάλειας ή ομαδοποιημένες πολιτικές που επιτρέπει ή απαγορεύει τα πακέτα, αφού έχει εξετάσει τις επικεφαλίδες των πακέτων και άλλες ιδιότητες. Κάθε δήλωση άδειας ή άρνησης στην ACL καλείται καταχώρηση ελέγχου πρόσβασης (access control entry - ACE). Οι καταχωρήσεις ελέγχου πρόσβασης μπορούν να ταξινομήσουν τα πακέτα επιθεωρώντας τις επικεφαλίδες μέχρι και το τέταρτο στρώμα πρωτοκόλλων, συμπεριλαμβανομένων των εξής:

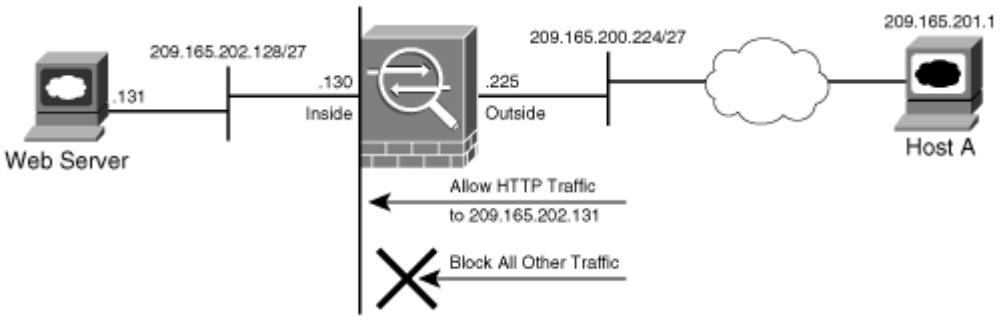
- Στρώμα 2 - πληροφορίες πρωτοκόλλου όπως EtherType
- Στρώμα 3 - πληροφορίες πρωτοκόλλου όπως ICMP, TCP ή UDP
- Διευθύνσεις IP πηγής και προορισμού
- Θύρες TCP ή UDP πηγής και προορισμού

Όταν μια λίστα ελέγχου πρόσβασης έχει διαμορφωθεί κατάλληλα, μπορεί να εφαρμοστεί σε μια διεπαφή για να φιλτράρει την κυκλοφορία. Η συσκευή ασφάλειας μπορεί να φιλτράρει τα πακέτα σε μια διεπαφή στην εισερχόμενη και στην εξερχόμενη κατεύθυνση. Όταν σε μια διεπαφή εφαρμόζεται μια εισερχόμενη ACL, η συσκευή ασφάλειας επιθεωρεί τα πακέτα ενάντια στις ACE αφού τα λάβει ή πριν τα διαβιβάσει. Εάν ένα πακέτο επιτρέπεται, η συσκευή ασφάλειας συνεχίζει να το επεξεργάζεται, προωθώντας το σε άλλες μηχανές διαμορφώσεις. Εάν ένα πακέτο απαγορεύεται από την ACL, η συσκευή ασφάλειας απορρίπτει το πακέτο και παράγει ένα μήνυμα syslog που δείχνει ότι ένα τέτοιο γεγονός έχει εμφανιστεί. Στο σχήμα 7-1, στην εξωτερική διεπαφή έχει εφαρμοστεί μια εισερχόμενη ACL που επιτρέπει μόνο την HTTP κυκλοφορία που προορίζεται για την IP 209.165.202.131. Η υπόλοιπη κυκλοφορία στη διεπαφή θα απορρίπτεται.



Σχήμα 7-1 : Εισερχόμενο φιλτράρισμα πακέτων

Εάν σε μια διεπαφή εφαρμόζεται μια εξερχόμενη ACL, η συσκευή ασφάλειας επεξεργάζεται τα πακέτα μέσω των διαφορετικών διαδικασιών (NAT, QoS, VPN) και έπειτα εφαρμόζει τις ACE που έχουν διαμορφωθεί. Η συσκευή ασφάλειας διαβιβάζει τα πακέτα μόνο εάν επιτρέπονται για αποστολή. Εάν τα πακέτα αμφισβητούνται ακόμη από και μια καταχώρηση, η συσκευή ασφάλειας απορρίπτει τα πακέτα και παράγει ένα μήνυμα syslog που δείχνει ότι ένα τέτοιο γεγονός έχει εμφανιστεί. Στο σχήμα 7-2, στην εσωτερική διεπαφή έχει εφαρμοστεί μια εξερχόμενη ACL που επιτρέπει μόνο την κυκλοφορία HTTP που προορίζεται για την IP 209.165.202.131. Η υπόλοιπη κυκλοφορία που θα προσπαθήσει να περάσει μέσω της συσκευής ασφάλειας, προς το εσωτερικό δίκτυο θα απορρίπτεται.



Σχήμα 7-2 : Εξερχόμενο φιλτράρισμα πακέτων

7.3 Κατηγορίες ACL

Η συσκευή ασφάλειας υποστηρίζει πέντε διαφορετικούς τύπους ACL, παρέχοντας μια ευέλικτη και επεκτάσιμη λύση στο φιλτράρισμα των μη εξουσιοδοτημένων πακέτων στο δίκτυο:

1. Τυπική ACL
2. Εκτεταμένη ACL
3. IPv6 ACL
4. EtherType ACL
5. WebVPN ACL

Τυπική ACL: Οι τυπική ACL (standard ACL) χρησιμοποιείται για να προσδιορίσει τα πακέτα με βάση τις IP διευθύνσεις προορισμού. Ένα από τα σενάρια που μπορούν να χρησιμοποιηθούν αυτού του τύπου ACL είναι ο διαχωρισμός σηράγγων (split tunneling) για απομακρυσμένης πρόσβασης VPN και αναδιανομή δρομολόγησης (route redistribution). Ωστόσο, δεν μπορούν να εφαρμοστούν σε μια διεπαφή για φιλτράρισμα πακέτων. Μια τυπική ACL μπορεί να χρησιμοποιηθεί μόνο εάν η συσκευή ασφάλειας τρέχει σε κατάσταση δρομολόγησης.

Εκτεταμένη ACL: Οι εκτεταμένες ACL (extended ACL), που είναι και οι πιο διαδεδομένες, μπορούν να ταξινομήσουν τα πακέτα βασισμένα στις ακόλουθες ιδιότητες:

- IP διευθύνσεις πηγής και προορισμού
- Πρωτόκολλα στρώματος 3
- Θύρες TCP και UDP πηγής ή/και προορισμού
- Τύπος προορισμού ICMP για τα πακέτα ICMP

Μια εκτεταμένη ACL μπορεί να χρησιμοποιηθεί για το φιλτράρισμα πακέτων διεπαφών, την ταξινόμηση πακέτων για QoS, τον προσδιορισμό πακέτων για NAT ή VPN κρυπτογράφηση και διάφορα άλλα χαρακτηριστικά γνωρίσματα. Αυτού του τύπου ACL μπορούν να χρησιμοποιηθούν στη συσκευή ασφάλειας σε κατάσταση δρομολόγησης αλλά και όταν λειτουργεί σε διαφανή κατάσταση.

IPv6 ACL: Μια ACL IPv6 λειτουργεί ομοίως με μια εκτεταμένη ACL. Ωστόσο, προσδιορίζει μόνο την κυκλοφορία τύπου IPv6 που περνά μέσω μιας συσκευής ασφάλειας σε κατάσταση δρομολόγησης.

EtherType ACL: Οι EtherType ACL μπορούν να χρησιμοποιηθούν στο να φιλτράρουν IP και μη IP κυκλοφορία, ελέγχοντας του πεδίο τύπου κώδικα Ethernet στην επικεφαλίδα του δεύτερου στρώματος. Η IP κυκλοφορία χρησιμοποιεί την τιμή τύπου κώδικα Ethernet 0x800, ενώ το IPX Novell χρησιμοποιεί 0x8137 ή 0x8138 ανάλογα με την έκδοση Netware. Μια ACL EtherType μπορεί να διαμορφωθεί μόνο εάν η συσκευή ασφάλειας λειτουργεί σε διαφανή κατάσταση.

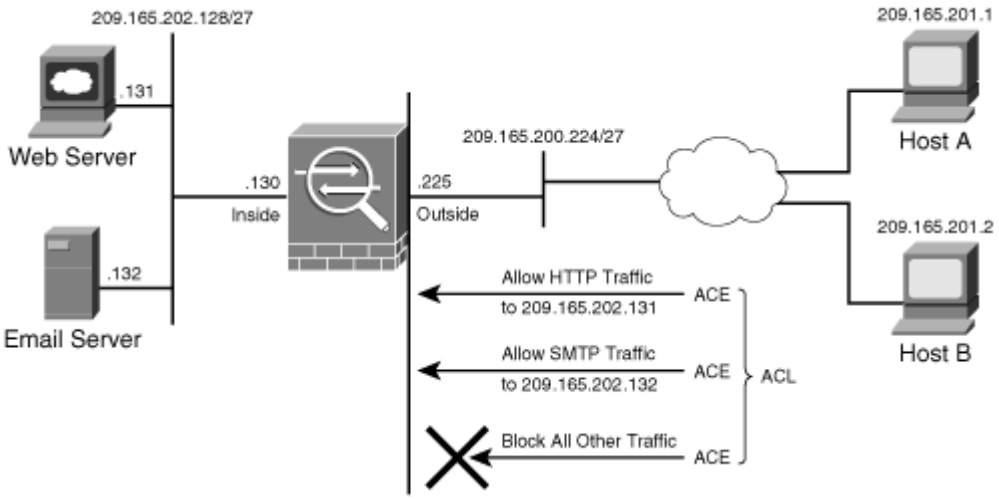
WebVPN ACL: Μια ACL WebVPN επιτρέπει τον περιορισμό της κυκλοφορίας που έρχεται μέσω των WebVPN τούνελ. Στην περίπτωση όπου έχει διαμορφωθεί μια ACL WebVPN αλλά δεν υπάρχει καμία αντιστοιχία για ένα πακέτο, η συμπεριφορά προεπιλογής πρόκειται να απορρίψει το πακέτο. Αφ' ετέρου, εάν δεν έχει καθοριστεί καμία ACL, η συσκευή ασφάλειας επιτρέπει στην κυκλοφορία να περάσει.

7.4 Διαμόρφωση φιλτραρίσματος πακέτων

Το φιλτράρισμα πακέτων απαιτεί τρία βήματα διαμόρφωσης:

- Βήμα 1: Δημιουργία ACL.
- Βήμα 2: Εφαρμογή της ACL σε μια διεπαφή.
- Βήμα 3: Δημιουργία ACL IPv6 (προαιρετικό).

Βήμα 1: Δημιουργία ACL. Μια ACL προσδιορίζει την κυκλοφορία που πρέπει να επιτραπεί ή να απορριφτεί. Μια ACE μπορεί να είναι απλή, όπως στην περίπτωση που επιτρέπει όλη την κυκλοφορία IP, ή περίπλοκη όπως στην περίπτωση που επιτρέπει την κυκλοφορία που προέρχεται από μια μοναδική IP διεύθυνση πηγής σε μια συγκεκριμένη θύρα και προορίζεται για μια άλλη συγκεκριμένη θύρα στη διεύθυνση προορισμού. Μια ACE καθορίζεται με τη χρησιμοποίηση της εντολής *access-list*. Για το φιλτράρισμα διεπαφών, μπορούμε να ορίσουμε μια εκτεταμένη ACL, μια ACL IPv6, ή μια ACL EtherType. Το σχήμα 7-3 περιέχει ένα web server και ένα e-mail server. Και οι δύο διακόμισες επιτρέπουν την κυκλοφορία που προορίζεται για την IP 209.165.202.131 με θύρα 80 (HTTP) και 209.165.202.132 με θύρα 25 (SMTP). Ωστόσο, η συσκευή ασφάλειας επιτρέπει σε μόνο δύο υπολογιστές πελάτες με IP 209.165.201.1 και 209.165.201.2 για να ξεκινήσουν την κυκλοφορία. Όλη η άλλη κυκλοφορία που περνά μέσω της συσκευής ασφάλειας θα απορρίπτεται.



Σχήμα 7-3 : Φιλτράρισμα εισερχομένης κυκλοφορίας

Το παράδειγμα 7-1 παρουσιάζει την διαμόρφωση για το σχήμα 7-3. Έχει δημιουργηθεί μια εκτεταμένη ACL με όνομα inbound_traffic_on_outside και τέσσερις εγγραφές ACE. Οι πρώτες δύο ACE επιτρέπουν την κυκλοφορία HTTP που προορίζεται για την IP 209.165.202.131 και προέρχεται από τους δύο υπολογιστές πελάτες, ενώ οι τελευταίες δύο ACE επιτρέπουν και στους δύο υπολογιστές την πρόσβαση SMTP για την IP 209.165.202.132. Προτείνεται η προσθήκη παρατηρήσεων σε μια ACL, επειδή βοηθά τους άλλους να αναγνωρίσουν την λειτουργία της. Σε αυτό το παράδειγμα έχουμε προσθέσει ως παρατήρηση το μήνυμα «This is the interface ACL to block inbound traffic». Γενικά, εάν δεν βρεθεί καμία ACE που θα επιτρέψει ρητά το πακέτο η συσκευή ασφάλειας θα το απορρίψει. Στο τέλος κάθε ACL υπάρχει ένας υπονοούμενος κανόνας που απαγορεύει όλα τα πακέτα (implicit deny).

Παράδειγμα 7-1 : Διαμόρφωση εκτεταμένης ACL
Fw1# configure terminal Fw1(config)# access-list inbound_traffic_on_outside remark This is the interface ACL to block inbound traffic Fw1(config)# access-list inbound_traffic_on_outside extended permit tcp host 209.165.201.1 host 209.165.202.131 eq www

Βήμα 2: Εφαρμογή της ACL σε μια διεπαφή. Το επόμενο βήμα μετά την διαμόρφωση μιας ACL είναι να εφαρμοστεί σε μια διεπαφή είτε στην εισερχόμενη είτε στην εξερχόμενη κατεύθυνση. Μπορούμε να εφαρμόσουμε μια ACL με τη χρησιμοποίηση της εντολής *access-group* σε συνδυασμό με το όνομα της ACL, όπως φαίνεται στην ακόλουθη σύνταξη:

access-group access-list {in | out} interface interface_name [per-user-override]

Ο πίνακας 7-1 απαριθμεί τα στοιχειά που χρησιμοποιούνται στην εντολή *access-group*.

Πίνακας 7-1 : Προσδιορισμός εντολής access-group	
Σύνταξη	*Περιγραφή*
access-group	Χρησιμοποιείται για να εφαρμόσει την ACL στη διεπαφή.

Πίνακας 7-1 : Προσδιορισμός εντολής access-group	
Σύνταξη	*Περιγραφή*
access-list	Το όνομα της ACL που εφαρμόζεται σε μια διεπαφή.
in	Η ACL θα εφαρμοστεί στην εισερχόμενη κατεύθυνση.
out	Η ACL θα εφαρμοστεί στην εξερχόμενη κατεύθυνση.
interface	Λέξη κλειδί για να διευκρινίσει τη διεπαφή στην οποία να εφαρμόσει η ACL.
interface_name	Το όνομα της διεπαφής στην οποία να εφαρμόσει η ACL.
per-user-override	Επιλογή που επιτρέπει στις αυτόματες ACL να αγνοήσουν τις καταχωρήσεις στην ACL διεπαφών.

Η συσκευή ασφάλειας δεν εμποδίζει την κυκλοφορία TCP ή UDP που επιστρέφει στη διεπαφή με χαμηλό επίπεδο ασφάλειας εάν η κυκλοφορία προέρχεται από έναν σύστημα στην διεπαφή με μεγαλύτερο επίπεδο ασφάλειας. Για άλλα πρωτόκολλα, όπως GRE ή ESP, θα πρέπει να επιτραπεί η επιστρεφόμενη κυκλοφορία με προσθήκη καταχώρισης στην ACL που εφαρμόζεται σε εκείνη την διεπαφή. Για το ICMP, μπορούμε είτε να επιτρέψουμε την κυκλοφορία μέσω ACL είτε να ενεργοποιήσουμε την επιθεώρηση ICMP. Στο παράδειγμα 7-2, μια ACL που ονομάζεται *inbound_traffic_on_outside* εφαρμόζεται στην εξωτερική διεπαφή με εισερχόμενη κατεύθυνση.

Παράδειγμα 7-2 : Εφαρμογή ACL στην εξωτερική διεπαφή
Fw1# configure terminal Fw1(config)# access-group inbound_traffic_on_outside in interface outside

Ανά κάθε κατεύθυνση μπορεί να εφαρμοστεί μονό μια εκτεταμένη ACL. Επιπρόσθετα υπάρχει η δυνατότητα να εφαρμοστεί μια εκτεταμένη και μια ACL IPv6 στην ίδια κατεύθυνση εάν η συσκευή ασφάλειας λειτουργεί σε κατάσταση δρομολόγησης. Σε διαφανή κατάσταση, στην ίδια κατεύθυνση μπορεί να εφαρμοστεί μια εκτεταμένη ACL και μια ACL EtherType.

Βήμα 3: Δημιουργία ACL IPv6. Όπως αναφέρθηκε παραπάνω η συσκευή ασφάλειας υποστηρίζει το φιλτράρισμα της κυκλοφορία IPv6. Μια ACL IPv6 καθορίζεται με τη χρησιμοποίηση της εντολής *ipv6 access-list* και ακολουθείται από το όνομα της ACL. Ο πίνακας 7-2 απαριθμεί τα στοιχειά που χρησιμοποιούνται σε μια ACE IPv6. Τα στοιχειά είναι διαφορετικά από αυτά που χρησιμοποιούνται στον πίνακα 7-1.

Πίνακας 7-2 : Προσδιορισμός IPv6 ACE	
Σύνταξη	*Περιγραφή*
ipv6	Λέξη κλειδί που χρησιμοποιείται για να δημιουργηθεί μια ACL IPv6.
source-ipv6-prefix	Δίκτυο ή IPv6 διεύθυνση πηγής.
prefix-length	Μάσκα δικτύου που εφαρμόζεται σε μια διεύθυνση IPv6.
source-ipv6-address	Ορίζει την IPv6 διεύθυνση πηγής που θα φιλτράρεται.
destination-ipv6-prefix	Δίκτυο ή διεύθυνση IPv6 που θα σταλεί το πακέτο.
destination-ipv6-address	Ορίζει την διεύθυνση προορισμού IPv6 που θα φιλτράρεται.
icmp6	Ορίζει ότι το πρωτόκολλο θα είναι ICMPv6.

Στο παράδειγμα 7-3, η ACL με όνομα inbound-ipv6-traffic-on-outside αποτελείται από δύο καταχωρίσεις ACE. Η πρώτη ACE απαγορεύει την κυκλοφορία που προέρχεται από την IPv6 διεύθυνση πηγής fedc:ba98:1:3210:fedc:ba98:1:3210 και προορίζεται για το mail server (θύρα TCP 25) και έχει διεύθυνση 1080::8:800:200c:417a. Η δεύτερη ACE επιτρέπει όλη την κυκλοφορία ταχυδρομείου από το δίκτυο fedc:ba98:1:3210::/64 εάν προορίζεται για 1080::8:800:200c:417a. Η ACL εφαρμόζεται στην εξωτερική διεπαφή στην εισερχόμενη κατεύθυνση.

Παράδειγμα 7-3 : Διαμόρφωση και εφαρμογή ACL IPv6
Fw1# configure terminal Fw1(config)# ipv6 access-list inbound-ipv6-traffic-on-outside permit tcp host fedc:ba98:1:3210:fedc:ba98:1:3210 host 1080::8:800:200c:417a eq smtp Fw1(config)# ipv6 access-list inbound-ipv6-traffic-on-outside permit tcp edc:ba98:1:3210::/64 host 1080::8:800:200c:417a eq smtp Fw1(config)# access-group inbound-ipv6-traffic-on-outside in interface outside

7.5 Έλεγχος ACL

Για να διαπιστωθεί εάν τα πακέτα περνούν μέσω των διαμορφωμένων ACL θα πρέπει να χρησιμοποιηθεί η εντολή *show access-list*. Όταν ένα πακέτο αντιστοιχείται ενάντια σε μια ACE, ο μετρητής *hitcnt* (hit count) αυξάνετε κατά ένα. Αυτό είναι χρήσιμο όταν θέλουμε να προσδιορίσουμε εάν η κυκλοφορία χρησιμοποίει μια διαμορφωμένη ACE. Είναι επίσης χρήσιμο για να ελέγξει εάν τα πακέτα επιτρέπονται ή απορρίπτονται. Το παράδειγμα 7-4 παρουσιάζει τη διαμόρφωση μιας ACL με όνομα *outside_in* και την έξοδο της εντολής *show access-list outside_in*. Όπως είναι εμφανής στο παράδειγμα, η συσκευή ασφάλειας επεξεργάστηκε 1009 πακέτα που αμφισβητήθηκαν και καταγράφηκαν από τις ACE. Για να μηδενιστούν οι μετρητές θα πρέπει να εκτελεστεί η εντολή *clear access-list* ακολουθουμένη από το όνομα της ACL

Παράδειγμα 7-4 : Αποτελέσματα εντολής show access-list outside_in
Fw1(config)# show running-config access-list outside_in access-list outside_in remark ACL to block inbound traffic on the outside interface access-list outside_in extended permit tcp any object-group DMZ_Web_Servers eq www access-list outside_in extended permit tcp any object-group DMZ_Email_Servers eq smtp access-list outside_in extended deny ip any any log

```
Fw1(config)# show access-list outside_in
access-list outside_in; 6 elements
access-list outside_in line 1 remark ACL to block inbound traffic on the outside interface
access-list outside_in line 2 extended permit tcp any object-group DMZ_Web_Servers eq www
access-list outside_in line 2 extended permit tcp any host 209.165.201.10 eq www (hitcnt=9)
access-list outside_in line 2 extended permit tcp any host 209.165.201.11 eq www (hitcnt=100)
access-list outside_in line 2 extended permit tcp any host 209.165.201.12 eq www (hitcnt=24)
access-list outside_in line 3 extended permit tcp any object-group DMZ_Email_Servers eq smtp
access-list outside_in line 3 extended permit tcp any host 209.165.201.20 eq smtp (hitcnt=3)
access-list outside_in line 3 extended permit tcp any host 209.165.201.21 eq smtp
(hitcnt=199)
access-list outside_in line 4 extended deny ip any any log informational interval 300 (hitcnt=1009)
```

Η συσκευή ασφάλειας μπορεί να ενεργήσει και ως sniffer για να συγκεντρώσει πληροφορίες για τα πακέτα που περνούν μέσω των διεπαφών. Αυτό το χαρακτηριστικό είναι σημαντικό όταν χρειάζεται να επιβεβαιωθεί ότι η κυκλοφορία από έναν συγκεκριμένο υπολογιστή ή ένα δίκτυο φθάνει στις διεπαφές. Μπορούμε να χρησιμοποιήσουμε μια ACL για να προσδιορίσουμε τον τύπο της κυκλοφορίας και παράλληλα να την συνδέσουμε σε μια διεπαφή με τη χρησιμοποίηση της εντολής *capture*. Στο παράδειγμα 7-5 έχει διαμορφωθεί μια ACL με το όνομα *inside-capture*. Η συγκεκριμένη ACL θα προσδιορίσει τα πακέτα που ξεκινούν από την IP 209.165.202.130 και προορίζονται για την IP 209.165.200.230. Η συσκευή ασφάλειας χρησιμοποιεί

την ACL για να συλλάβει την προσδιορισμένη κυκλοφορία στην εσωτερική διεπαφή χρησιμοποιώντας έναν κατάλογο σύλληψης που ονομάζεται cap-inside.

Για να προβάλλουμε τα πακέτα, χρησιμοποιούμε την εντολή show capture ακολουθουμένη από το όνομα του καταλόγου καταγραφής. Στο παράδειγμα 7-5 η συσκευή ασφάλειας συνέλαβε 15 πακέτα που συμφωνούν με την ACL στην εσωτερική διεπαφή. Η παρακάτω έξοδος δείχνει ένα πακέτο TCP SYN που προέρχεται από την IP 209.165.202.130 με θύρα πηγής 11084 και προορίζεται για την IP 209.165.200.230 και θύρα 23. Το μέγεθος παραθύρων TCP είναι 4128 ενώ το μέγιστο μέγεθος τμήματος (Maximum Segment Size - MSS) έχει οριστεί στα 536 byte.

Παράδειγμα 7-5 : Καταγραφή πακέτων

```
Fw1(config)# access-list inside-capture permit ip host 209.165.202.130 host 209.165.200.230
Fw1(config)# capture cap-inside access-list inside-capture interface inside

Fw1(config)# show capture cap-inside
15 packets captured
1: 02:12:47.142189 209.165.202.130.11084 > 209.165.200.230.23: S 433720059:433720059(0) win 4128 <mss 536>
 2: 02:12:47.163489 209.165.202.130.11084 > 209.165.200.230.23:. ack 1033049551 win 4128
….
….
15 packets shown
```

Η έξοδος της εντολής *capture* μπορεί να αποθηκευτή σε μορφή pcap και στη συνεχεία να εισαχθεί σε ένα εργαλείο sniffing όπως τα Ethereal και TCPDUMP για περαιτέρω ανάλυση.

ΚΕΦΑΛΑΙΟ 8
Επικύρωση Έγκριση Παρακολούθηση

8.1 Εισαγωγή

Οι συσκευές ασφάλειας χρειάζεται να έχουν δυνατότητες για πιστοποίηση της ταυτότητας του χρήστη, τη παροχή ή όχι πρόσβασης και την παρακολούθηση των κινήσεων των απομακρυσμένων χρηστών αντίστοιχα. Για να ανταποκριθούν στα παραπάνω, χρησιμοποιούν μία στρατηγική που είναι γνωστή ως επικύρωση, έγκριση και παρακολούθηση (authentication, authorization, accounting - AAA). Στα σημερινά δίκτυα για την παροχή AAA λύσεων χρησιμοποιούνται τα πρωτοκολλά TACACS+ (Terminal Access Controller Access Control System plus) και RADIUS (Remote Access Dial-In User Service). Αυτό το κεφάλαιο αναλύει την διαμόρφωση των υπηρεσιών AAA.

8.2 Εισαγωγή στο AAA

Επικύρωση: Είναι η διαδικασία πιστοποίησης των χρηστών με βάση την ταυτότητά τους και κάποια προκαθορισμένα χαρακτηριστικά, όπως οι κωδικοί πρόσβασης και τα ψηφιακά πιστοποιητικά. Οι συνήθεις μέθοδοι έγκρισης χρησιμοποιούν μια βάση δεδομένων που αποτελείται από όνομα χρηστή και κωδικό στον διακομιστή πρόσβασης. Πιο εξελιγμένα συστήματα χρησιμοποιούν μεθόδους όπως το TACACS και το Kerberos. Ωστόσο, το ότι πιστοποιείται η ταυτότητα κάποιου χρήστη δε σημαίνει αυτόματα ότι έχει αποκτήσει και πρόσβαση σε όλες τις υπηρεσίες του δικτύου. Είναι πιθανό να του ζητηθεί εκ νέου κωδικός από κάποια συγκεκριμένη υπηρεσία όπως UNIX, NetWare ή AppleShare.

Έγκριση: Είναι η μέθοδος του περιορισμού των δικτυακών υπηρεσιών σε διαφορετικούς χρήστες βάση μιας δυναμικά εφαρμοζόμενης λίστας πρόσβασης που μερικές φορές αναφέρεται και ως "προφίλ χρήστη" και βασίζεται στο δίδυμο username/password. Με αλλά λόγια η έγκριση αποτελεί την απάντηση στα δικαιώματα έχει ένας χρηστής και τις ενέργειες μπορεί να κάνει στο δίκτυο.

Παρακολούθηση: Είναι η διαδικασία της συγκέντρωσης πληροφοριών από τους χρήστες και αποστολής τους σε έναν κεντρικό υπολογιστή AAA, χρησιμοποιώντας τους χρόνους σύνδεσης (όταν ο χρήστης συνδέεται και αποσυνδέεται από το σύστημα) και τις υπηρεσίες όπου οι χρήστες έχουν πρόσβαση. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για την τιμολόγηση, τον έλεγχο, και την υποβολή εκθέσεων.

8.3 Πρωτόκολλα και υπηρεσίες AAA

Μια συσκευή ασφάλειας μπορεί να διαμορφωθεί κατά τρόπο που να διατηρήσει μια τοπική βάση δεδομένων χρηστών ή να χρησιμοποιήσει έναν εξωτερικό κεντρικό υπολογιστή. Παρακάτω παρουσιάζονται τα AAA πρωτοκόλλα που μπορούν να χρησιμοποιηθούν σαν απομακρυσμένες βάσεις δεδομένων:

- RADIUS
- TACACS+
- RSA SecurID (SDI)
- Windows NT
- Kerberos
- Lightweight Directory Access Protocol (LDAP)

Το πρωτόκολλο RADIUS αναπτύχθηκε από την Livingston Enterprises ως ένας server πρόσβασης, πιστοποίησης και παρακολούθησης. Από τότε έχει υλοποιηθεί από διάφορους άλλους πωλητές και έχει κερδίσει ευρεία υποστήριξη ανάμεσα ακόμα και στους παροχείς υπηρεσιών (ISPs). Το RADIUS είναι βασισμένο στο μοντέλο client/server. Οι servers πρόσβασης (NAS-Network

Access Servers) λειτουργούν σαν clients του RADIUS. Ο client είναι υπεύθυνος για την προώθηση της πληροφορίας του χρήστη στον αρμόδιο RADIUS server και την εκτέλεση των εντολών που θα του σταλούν πίσω από το server. Ο RADIUS server ή daemon παρέχει υπηρεσίες πιστοποίησης και παρακολούθησης σε έναν ή περισσότερους RADIUS clients δηλαδή συσκευές NAS. Οι RADIUS servers είναι υπεύθυνοι για το να λαμβάνουν τις αιτήσεις σύνδεσης των χρηστών, να τους πιστοποιούν και τέλος να επιστρέφουν όλη τη πληροφορία με τις απαιτούμενες ρυθμίσεις για τους clients, ώστε να δοθούν οι αιτούμενες υπηρεσίες στους χρήστες. Ο RADIUS server πρόσβασης είναι συνήθως ένας αφιερωμένος σταθμός εργασίας συνδεδεμένος με το δίκτυο.

Το πρωτόκολλο TACACS+ επιτρέπει σε ένα ξεχωριστό server πρόσβασης να παρέχει υπηρεσίες πιστοποίησης, έγκρισης και παρακολούθησης με ανεξάρτητο τρόπο. Κάθε υπηρεσία μπορεί να συνδυαστεί με τη δική της βάση δεδομένων ή να χρησιμοποιήσει άλλες υπηρεσίες που είναι διαθέσιμες στο δίκτυο. Η φιλοσοφία σχεδίασης του TACACS+ βασίζεται στο καθορισμό μιας μεθόδου για την διαχείριση μη όμοιων server πρόσβασης (NAS) από ένα και μόνο σύνολο διαχειριστικών υπηρεσιών. Ένας NAS παρέχει πρόσβαση σε έναν χρήστη, σε ένα δίκτυο ή υποδίκτυο ή και σε διασυνδεδεμένα δίκτυα. Το TACACS+ αποτελείται από τρία κύρια μέρη: την υποστήριξη του πρωτοκόλλου από servers πρόσβασης και δρομολογητές, τα χαρακτηριστικά του πρωτοκόλλου και την κεντρική βάση δεδομένων. Παρόμοια με μια εσωτερική βάση δεδομένων, το TACACS+ υποστηρίζει τα απαιτούμενα χαρακτηριστικά ενός ασφαλούς συστήματος. Ο πίνακας 8-1 παρουσιάζει τις μεθόδους και λειτουργίες που υποστηρίζει το κάθε πρωτόκολλο.

Πίνακας 8-1 : Χαρακτηριστικά πρωτοκόλλων AAA

Μέθοδος	*Authentication*	*Authorization*	*Accounting*
Τοπικά	Ναι	Ναι	Όχι
RADIUS	Ναι	Ναι	Ναι
TACACS+	Ναι	Ναι	Ναι

Πίνακας 8-1 : Χαρακτηριστικά πρωτοκόλλων ΑΑΑ			
Μέθοδος	*Authentication*	*Authorization*	*Accounting*
SDI	Ναι	Όχι	Όχι
Windows NT	Ναι	Όχι	Όχι
Kerberos	Ναι	Όχι	Όχι
LDAP	Όχι	Ναι	Όχι

8.4 Καθορισμός εξυπηρετητή επικύρωσης

Πριν τη διαμόρφωση ενός εξυπηρετητή επικύρωσης (authentication server), πρέπει να διευκρινιστούν οι ομάδες εξυπηρετητών ΑΑΑ με την εντολή *aaa-server*. Η σύνταξη της εντολής aaa-server διευκρινίζει μια νέα ομάδα εξυπηρετητών ΑΑΑ και το αντίστοιχο πρωτόκολλο: *aaa-server server-tag protocol server-protocol.*

Παράδειγμα 8-1: Πρωτόκολλα επικύρωσης και ομάδες εξυπηρετητών ΑΑΑ
Fw1(config)# aaa-server mygroup protocol radius

Για να ορίσουμε τους εξυπηρετητές ΑΑΑ που ανήκουν στις συγκεκριμένες ομάδες, χρησιμοποιούμε την ακόλουθη εντολή: *aaa-server server-tag host ip_address*. Το παράδειγμα 8-2 παρουσιάζει μια διαμόρφωση με δύο εξυπηρετητές που ανήκουν στην ομάδα εξυπηρετητών με όνομα mygroup.

Παράδειγμα 8-2. Διαμόρφωση εξυπηρετητών ΑΑΑ
Fw1# configure terminal Fw1(config)# aaa-server mygroup host 172.18.124.11 Fw1(config-aaa-server)# retry-interval 3 Fw1(config-aaa-server)# timeout 30 Fw1(config-aaa-server)# key pass123 Fw1(config-aaa-server)# exit

```
Fw1(config)# aaa-server mygroup host 172.18.124.12
Fw1(config-aaa-server)# retry-interval 3
Fw1(config-aaa-server)# timeout 30
Fw1(config-aaa-server)# key pass123
Fw1(config-aaa-server)# exit
```

Για να ελέγξουμε τις στατιστικές για όλους τους εξυπηρετητές AAA που καθορίζονται για ένα συγκεκριμένο πρωτόκολλο, χρησιμοποιούμε την ακόλουθη εντολή: *show aaa-server protocol server-protocol* .

8.5 Επικύρωση συνόδων διαχείρισης

Η συσκευή ασφάλειας ASA υποστηρίζει την επικύρωση των συνόδων διαχείρισης χρησιμοποιώντας είτε την τοπική βάση δεδομένων χρηστών, είτε ένα RADIUS εξυπηρετητή ή ένα TACACS+ εξυπηρετητή. Ο διαχειριστής μπορεί να συνδεθεί με την συσκευή ασφάλειας μέσω :

- Telnet
- Secure Shell (SSH)
- Serial console
- Cisco ASA Device Manager (ASDM)

Εάν η σύνδεση πραγματοποιηθεί μέσω Telnet ή SSH, σε περίπτωση λάθους ο χρήστης μπορεί να ξαναδοκιμάσει την επικύρωση τρεις φορές. Μετά από την τρίτη φορά, η σύνοδος και η σύνδεση επικύρωσης θα κλείσουν. Οι σύνοδοι επικύρωσης μέσω της κονσόλας προτρέπουν το χρήστη συνεχώς έως ότου πληκτρολογούνται το σωστοί όνομα χρήστη και ο προσωπικός κωδικός. Παρακάτω παρουσιάζεται αναλυτικά η διαμόρφωση της επικύρωσης για κάθε τύπο σύνδεσης.

8.5.1 Επικύρωση για συνδέσεις μέσω Telnet

Η πρόσβαση μέσω Telnet μπορεί να επιτραπεί σε οποιαδήποτε εσωτερική ή εξωτερική διεπαφή. Οι σύνοδοι Telnet επιτρέπονται στην εξωτερική διεπαφή μόνο μέσα από μια σύνδεση IPSec. Το παράδειγμα 8-3 περιλαμβάνει τις απαραίτητες εντολές για να διαμορφώσουν την πρόσβαση μέσω Telnet χρησιμοποιώντας ένα τοπικό όνομα χρήστη και έναν κωδικό πρόσβασης.

Παράδειγμα 8-3 : Επικύρωση για σύνδεση Telnet
Fw1# configure terminal
Fw1(config)# username admin password pass123
Fw1(config)# aaa authentication telnet console LOCAL
Fw1(config)# telnet 192.168.10.0 255.255.255.0 inside
Fw1(config)# exit

Στο παράδειγμα 8.3, ο χρήστης με όνομα admin θα είναι σε θέση να επικυρωθεί επιτυχώς κατά τη σύνδεση μέσω Telnet στην εσωτερική διεπαφή μόνο αν προέρχεται από το δίκτυο 192.168.10.0/24. Η λέξη κλειδί *LOCAL* χρησιμοποιείται για να διευκρινίσει ότι θα χρησιμοποιηθεί η τοπική βάση δεδομένων χρηστών. Επίσης εφαρμόζεται για να επιτρέψει την επαναφορά στην τοπική βάση δεδομένων εάν ο διαμορφωμένος εξυπηρετητής επικύρωσης δεν είναι διαθέσιμος. Η λέξη κλειδί console χρησιμοποιείται για να αναγκάσει την συσκευή ασφάλειας να απαιτήσει την AAA για οποιοδήποτε χρήστη που προσπαθεί να συνδέσει με Telnet, serial console, HTTP, ή SSH.

8.5.2 Επικύρωση για συνδέσεις μέσω SSH

Για να ενεργοποιηθεί το πρωτόκολλο SSH, θα πρέπει πρώτα να διαμορφωθεί ένα όνομα host και domain και στη συνεχεία να γίνει η παραγωγή του κλειδιού RSA. Το παράδειγμα 8-4 δείχνει τον τρόπο δημιουργίας του κλειδιού RSA και την ενεργοποίηση της δεύτερης έκδοσης του SSH για συνδέσεις από οποιαδήποτε σύστημα στην εσωτερική διεπαφή.

Παράδειγμα 8-4 : Παραγωγή κλειδιού RSA , ενεργοποίηση SSH Version 2
Fw1# configure terminal Fw1(config)# hostname ASA Fw1(config)# domain-name cisco.com Fw1(config)# crypto key generate rsa modulus 2048 INFO: The name for the keys will be: ASA.cisco.com Keypair generation process begin. … Fw1(config)# ssh 0.0.0.0 0.0.0.0 inside Fw1(config)# ssh version 2

Μετά από τα παραπάνω βήματα, θα πρέπει να γίνει διαμόρφωση για τους εξυπηρετητές AAA . Στο παράδειγμα 8-5, ο εξυπηρετητής που διαμορφώνεται για την επικύρωση χρησιμοποιεί το πρωτόκολλο TACACS+ και η ομάδα εξυπηρετητών AAA θα ονομάζεται *mygroup*. Η διεύθυνση IP του εξυπηρετητή TACACS+ είναι 172.18.173.109 και διαμορφώνεται με κοινό μυστικό κλειδί το *pass123*.

Παράδειγμα 8-5 : Διαμόρφωση SSH επικύρωσης μέσω TACACS +
Fw1# configure terminal Fw1(config)# aaa-server mygroup protocol tacacs+ Fw1(config-aaa-server)# max-failed-attempts 2 Fw1(config-aaa-server)# reactivation-mode timed Fw1(config-aaa-server)# exit Fw1(config)# aaa-server mygroup host 172.18.173.109 Fw1(config-aaa-server)# key pass123 Fw1(config-aaa-server)# exit Fw1(config)# aaa authentication ssh console mygroup Fw1(config)# exit

8.5.3 Επικύρωση για συνδέσεις μέσω κονσόλας

Για να διαμορφωθεί η επικύρωση μέσω κονσόλας, θα πρέπει να χρησιμοποιηθεί η εντολή *aaa authentication serial console*. Το παράδειγμα 8-6 παρουσιάζει πώς μπορεί να διαμορφωθεί η επικύρωση για συνδέσεις μέσω κονσόλας, χρησιμοποιώντας την ομάδα κεντρικών εξυπηρετητών AAA που δημιουργήθηκε προηγουμένως.

Παράδειγμα 8-6 : Επικύρωση για σύνδεση μέσω κονσόλας
Fw1(config)# aaa authentication serial console mygroup

8.5.4 Επικύρωση για συνδέσεις μέσω ASDM

Η εντολή *aaa authentication http console* διαμορφώνεται για να απαιτήσει επικύρωση στους χρήστες που θέλουν να κάνουν διαχείριση μέσω ASDM. Το παράδειγμα 8-7 δείχνει πώς μπορεί να διαμορφωθεί η επικύρωση για HTTP συνδέσεις μέσω ASDM, χρησιμοποιώντας την ομάδα κεντρικών εξυπηρετητών AAA που δημιουργήθηκε προηγουμένως. Εάν η εντολή δεν ενεργοποιηθεί, τότε οι χρήστες ASDM μπορούν να αποκτήσουν πρόσβαση με την είσοδο μόνο του κωδικού ενεργοποίησης και η υπαγόρευση επικύρωσης δεν θα τους ζητήσει κανένα όνομα χρήστη.

Παράδειγμα 8-7 : Επικύρωση HTTP για σύνδεση μέσω ASDM
Fw1(config)# aaa authentication http console mygroup

8.6 Διαμόρφωση έγκρισης

Η συσκευές ασφάλειας PIX και ASA υποστηρίζουν υπηρεσίες έγκρισης μέσω TACACS+ για την αντιπυρική ζώνη πληρεξούσιου. Επίσης υποστηρίζουν υπηρεσίες έγκρισης για TACACS+ και την εσωτερική βάση δεδομένων χρηστών για τις συνόδους διαχείρισης. Άλλη μια λειτουργία που παρέχεται είναι

οι αυτόματες ACL μέσω RADIUS. Επιπλέον, για τις συνδέσεις χρηστών VPN η έγκριση μπορεί να πραγματοποιηθεί μέσω RADIUS, LDAP και τις εσωτερικές βάσεις δεδομένων. Η εντολή aaa authorization επιτρέπει την έγκριση για λειτουργίες αντιπυρικής ζώνη πληρεξούσιου και των συνόδων διαχείρισης και ακλουθεί την παρακάτω σύνταξη: *aaa authorization include | exclude svc if_name l_ip l_mask [f_ip f_mask]server_tag.* Το παράδειγμα 8-8 περιγράφει τον τρόπο χρήσης της εντολής. Η λίστα έλεγχου πρόσβασης με αριθμό 100 επιβάλει έγκριση στην κυκλοφορία IP που προέρχεται από το δίκτυο 10.10.10.0/24 και προορίζεται στο 192.168.1.0/24. Η συγκεκριμένη ACL συνδέεται με την εντολή *aaa authorization match*.

Παράδειγμα 8-8 : Ενεργοποίηση έγκρισης και καθορισμός κυκλοφορίας
access-list 100 extended permit ip 10.10.10.0 255.255.255.0 192.168.1.0 255.255.255.0 aaa-server mygroup protocol tacacs+ aaa-server mygroup host 10.10.10.100 key pass123 aaa authorization match 100 inside mygroup

Εντολή έγκρισης: Για να διαμορφωθεί η εντολή έγκρισης, χρησιμοποιείται η ακόλουθη εντολή: *aaa authorization command {LOCAL | tacacs_server_tag [LOCAL]}* . Η επιλογή server tag LOCAL καθορίζει την τοπική έγκριση. Μπορεί επίσης να χρησιμοποιηθεί ως μέθοδος ανάνηψης σε περίπτωση που για οποιοδήποτε λόγο ο εξυπηρετητής TACACS+ είναι εκτός λειτουργίας.

Διαμόρφωση αυτόματης ACL: Η συσκευή ασφάλειας παρέχει υποστήριξη έγκριση ACL ανά χρήστη με φόρτωση της ACL από ένα εξυπηρετητή RADIUS ή TACACS+. Το συγκεκριμένο γνώρισμα επιτρέπει την προώθηση μιας ACL στην αντιπυρική ζώνη από κάποιο εξυπηρετητή ACS. Η αυτόματη ACL θα λειτουργήσει σε συνδυασμό με τις ACL που είναι από πριν διαμόρφωνες. Για να επιτραπεί η κυκλοφορία θα πρέπει να επιτρέπεται και από τις δύο ACL. Ωστόσο, η επιλογή της ιδιότητας *per-user-override* στο τέλος της εντολής *access-group* μπορεί να παρακάμψει αυτή την απαίτηση. Όλες οι αυτόματες

ACL εφαρμόζονται στη διεπαφή από την οποία ο επικυρώνεται χρήστης. Στο παράδειγμα 8-9 εφαρμόζεται η επιλογή per-user-override στην εντολή *access-group* που με τη σειρά της συνδέεται με την εσωτερική διεπαφή:

Παράδειγμα 8-9 : Επιλογή per-user-override
access-group 100 in interface inside per-user-override

8.7 Διαμόρφωση παρακολούθησης

Για την διαμόρφωση της παρακολούθησης, χρησιμοποιείται η εντολή *aaa accounting*. Το παράδειγμα 8-10 παρουσιάζει τον τρόπο διαμόρφωσης της παρακολούθησης. Η λίστα έλεγχου πρόσβασης με αριθμό 100 δημιουργείται για να επιτρέψει την παρακολούθηση για όλες τις συνδέσεις που προέρχονται από το δίκτυο 10.1.1.0/24 και έχουν προορισμό το δίκτυο 172.18.124.0/24. Στη συνεχεία η ACL εφαρμόζεται στην εντολή *aaa accounting match*.

Παράδειγμα 8-10 : Ενεργοποίηση παρακολούθησης
Fw1(config)# access-list 100 permit ip 10.1.1.0 255.255.255.0 172.18.124.0 255.255.255.0 Fw1(config)# aaa accounting match 100 inside mygroup

8.8 Ανίχνευση λαθών AAA

Οι συνδέσεις διαχείρισης μπορούν να επικυρωθούν χρησιμοποιώντας RADIUS, TACACS+ ή την τοπική βάση δεδομένων χρηστών. Για την ανίχνευση των λαθών και προβλημάτων που μπορεί να προκύψουν κατά την προσπάθεια σύνδεσης χρησιμοποιούνται οι παρακάτω εντολές *debug* :

- debug aaa: Παρέχει τις πληροφορίες για την επικύρωση, την έγκριση, ή τα μηνύματα παρακολούθησης που παράγονται και λαμβάνονται.

- debug radius: Ανιχνεύει τα λάθη από τις συναλλαγές RADIUS και έχει τις ακόλουθες επιλογές:
- all: Ενεργοποιεί όλες τις επιλογές
- decode: Παρουσιάζει αποκωδικοποιημένα μηνύματα συναλλαγής RADIUS
- session: Παρέχει πληροφορίες για όλες τις συνόδους RADIUS
- user: Επιτρέπει τον έλεγχο των πληροφοριών συναλλαγής RADIUS για μια συγκεκριμένη σύνδεση χρηστών
- debug tacacs: Ανιχνεύει τα λάθη από τις συναλλαγές TACACS+ και έχει τις ακόλουθες επιλογές:
- session: Παρέχει πληροφορίες για όλες τις συνόδους TACACS+
- user: Επιτρέπει τον έλεγχο των πληροφοριών συναλλαγής TACACS+ για μια συγκεκριμένη σύνδεση χρηστών

ΚΕΦΑΛΑΙΟ 9
Δρομολόγηση

9.1 Εισαγωγή

Απόφαση δρομολόγησης είναι η διαδικασία όπου μια συσκευή δικτύων προσδιορίζει ποια διεπαφή και πύλη (gateway) πρέπει να χρησιμοποιηθεί για να διαβιβάσει τα πακέτα προς ένα συγκεκριμένο προορισμό. Η παρούσα απόφαση μπορεί να ληφθεί με τη χρησιμοποίηση δυναμικών πρωτοκόλλων δρομολόγησης ή στατικών καταχωρήσεων. Αυτό το κεφάλαιο καλύπτει τις δυνατότητες δρομολόγησης των συσκευών ασφάλειας ASA και PIX. Οι συσκευές ασφάλειας υποστηρίζουν στατική δρομολόγηση και τα πρωτοκόλλα RIP (Routing Information Protocol) και OSPF (Open Shortest Path First).

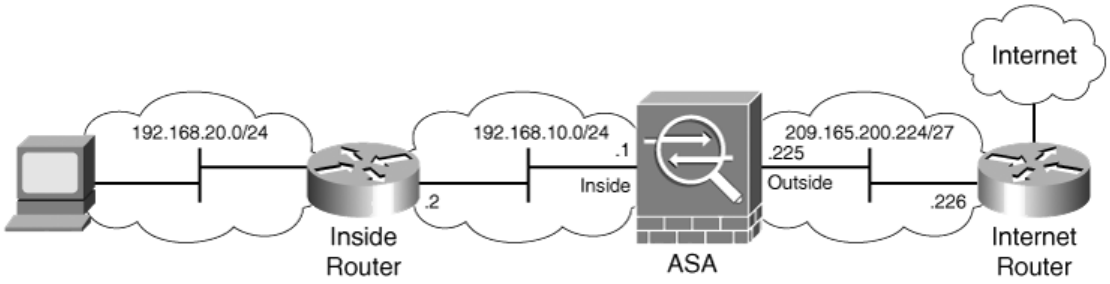
9.2 Διαμόρφωση στατικής δρομολόγησης

Η επέκταση και η διαμόρφωση της στατικής δρομολόγησης είναι κατάλληλη όταν δεν μπορεί να δημιουργηθεί δυναμικά μια δρομολόγηση προς ένα συγκεκριμένο προορισμό. Επιπλέον μπορεί να χρησιμοποιηθεί όταν η συσκευή στην οποία η συσκευή ασφάλειας διαβιβάζει τα πακέτα δεν υποστηρίξει τα δυναμικά πρωτόκολλα δρομολόγησης ή όταν το δίκτυο είναι μικρό και απλό. Τα δυναμικά πρωτόκολλα δρομολόγησης, όπως RIP και OSPF, πρέπει να εξεταστούν εάν το δίκτυο είναι αρκετά μεγάλο και σύνθετο. Η στατική δρομολόγηση είναι εύκολο να διαμορφωθεί. Ωστόσο, δεν μπορεί να επεκταθεί καλά σε μεγάλα περιβάλλοντα. Θα πρέπει να προηγηθεί η πλήρης κατανόηση της τοπολογίας των δικτύων πριν την διαμόρφωση της δρομολόγησης. Μια καλή πρακτική είναι να υπάρχει ένα διάγραμμα τοπολογίας δικτύων στο όποιο μπορούμε να αναφερθούμε κατά τη διάρκεια της διαμόρφωσης. Η στατική δρομολόγηση διαμορφώνεται χρησιμοποιώντας την εντολή *route*, όπως αναλύεται στο παράδειγμα 9-1, σε συνδυασμό με το αντίστοιχο πινάκα.

Παράδειγμα 9-1 : Διαμόρφωση στατικής δρομολόγησης
route interface network mask gateway metric [tunneled]

Πίνακας 9-1 : Επιλογές εντολής δρομολόγησης	
Επιλογή	*Περιγραφή*
interface	Το όνομα της διεπαφής που θα εφαρμοστεί η δρομολόγηση. Θα πρέπει να ταιριάξει με το όνομα της διεπαφής που έχει διαμορφωθεί από την εντολή nameif στα πλαίσια του συγκεκριμένου τμήματος διαμόρφωσης διεπαφών.
network	Η διεύθυνση του απομακρυσμένου δικτύου ή συστήματος. Εάν διαμορφώνουμε μια διαδρομή προεπιλογής, τότε η τιμή του δικτυού θα είναι 0.0.0.0 ή 0.
mask	Η μάσκα υποδικτύου για το απομακρυσμένου δικτύου. Εάν διαμορφώνουμε μια διαδρομή προεπιλογής, τότε η τιμή της μάσκας θα είναι 0.0.0.0 ή 0.
gateway	Η πύλη στην οποία το θα διαβιβαστούν τα πακέτα.
metric	Ο αριθμός των hops έως το δίκτυο προορισμού.
tunneled	Αυτή η επιλογή χρησιμοποιείται για να διαμορφώσει μια πύλη προεπιλογής σηράγγων. Μπορεί να χρησιμοποιηθεί μόνο με τις πύλες προεπιλογής.

Το σχήμα 9-1 παρουσιάζει μια απλή τοπολογία που περιλαμβάνει μια αντιπυρική ζώνη ASA με δύο διεπαφές (εξωτερική και εσωτερική) και στατική δρομολόγηση.



Σχήμα 9-1 : Στατική δρομολόγηση

Στο παράδειγμα που παρουσιάζεται στο σχήμα 9-1, για μπορέσει η συσκευή ασφάλειας ASA να διαβιβάσει τα πακέτα στο Διαδίκτυο μέσω του Internet router, θα πρέπει να διαμορφωθεί μια στατική δρομολόγηση προεπιλογής όπως δείχνει το παράδειγμα 9-2. Μπορούμε να διαμορφώσουμε μέχρι τρεις διαδρομές προεπιλογής για την εξισορρόπηση του φόρτου κυκλοφορίας, αλλά θα πρέπει όλες να εφαρμοστούν στην ίδια διεπαφή.

Παράδειγμα 9-2 : Στατική δρομολόγηση προεπιλογής
route outside 0.0.0.0 0.0.0.0 209.165.200.226 1

Το παράδειγμα 9-3 αποτελεί την στατική δρομολόγηση για να δρομολογηθούν τα πακέτα που προορίζονται στο ιδιωτικό δίκτυο 192.168.20.0/24.

Παράδειγμα 9-3 : Στατική δρομολόγηση
route inside 192.168.20.0 255.255.255.0 192.168.10.2 1

Η εντολή show route που εκτελείται στο παράδειγμα 9-4 χρησιμοποιείται για να εμφανίσει τον πίνακα δρομολόγησης και τον έλεγχο της τη διαμόρφωσης. Στην συγκειμένη περίπτωση εμφανίζει την έξοδο για της προηγούμενες εντολές στατικής δρομολόγησης. Το γράμμα S πριν από την δήλωση δρομολόγησης δείχνει ότι είναι μια στατική είσοδος δρομολόγησης. Το γράμμα C δείχνει ότι είναι μια άμεσα συνδεδεμένη διαδρομή. Ο πρώτος αριθμός σε παρένθεση είναι η διοικητική απόσταση (administrative distance) της πηγής πληροφοριών, ενώ ο δεύτερος αριθμός είναι το κόστος (metric) για τη διαδρομή. Η διοικητική απόσταση είναι το αναγνωριστικό που χρησιμοποιείται από το σύστημα δρομολόγησης για να επιλέξει την καλύτερη πορεία, όταν υπάρχουν δύο ή περισσότερες διαφορετικές διαδρομές προς το ίδιο προορισμό από δύο διαφορετικά πρωτόκολλα δρομολόγησης. Η εντολή show route είναι χρήσιμη κατά την ανίχνευση λαθών ή προβλημάτων δρομολόγησης. Παρέχει όχι μόνο την διεύθυνση IP της πύλης για κάθε είσοδο δρομολόγησης, αλλά και τη διεπαφή που συνδέεται με εκείνη την πύλη. Επίσης, μπορεί να χρησιμοποιηθεί με ένα όνομα διεπαφής προκειμένου να εμφανίσει μόνο την έξοδο δρομολόγησης της συγκεκριμένης διεπαφής.

Παράδειγμα 9-4 : Εντολή show route
Fw1# show route
S 0.0.0.0 0.0.0.0 [1/0] via 209.165.200.226, outside
C 192.168.10.0 255.255.255.0 is directly connected, inside
S 192.168.20.0 255.255.255.0 [1/0] via 192.168.10.2, inside
C 209.165.200.224 255.255.255.224 is directly connected, outside

9.3 Πρωτόκολλο πληροφοριών δρομολόγησης (RIP)

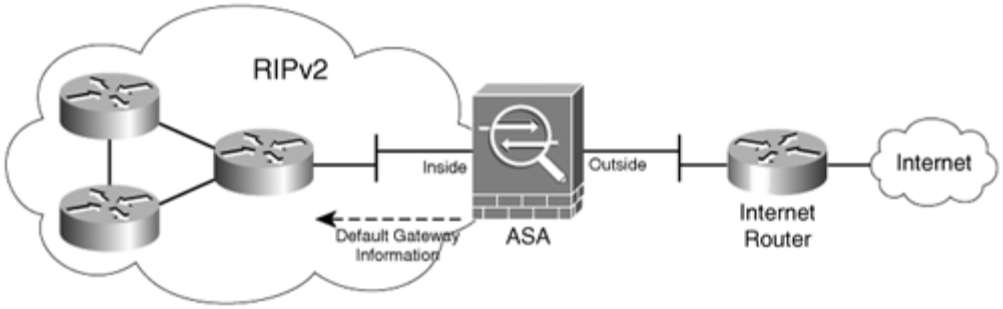
Το πρωτόκολλο πληροφοριών δρομολόγησης (Routing Information Protocol - RIP) ήταν από τα πρώτα πρωτοκόλλα δρομολόγησης που χρησιμοποιηθήκαν με το IP αλλά η εφαρμογή του συνεχίζεται ακόμη. Χρησιμοποιείται συνήθως σε μικρά και ομοιογενή δίκτυα. Το έγγραφο RFC 1058 περιγραφή την πρώτη έκδοση του RIP (RIP-1). Στα RFC 1721 και 1722 ορίζεται μια βελτιωμένη έκδοση, το RIP έκδοση 2 (RIP-2), που είναι πρωτόκολλο δρομολόγησης χωρίς κλάσεις. Τα βασικά χαρακτηριστικά του RIP είναι τα εξής :

- Δρομολόγηση μέσα σε ένα αυτόνομο σύστημα καθώς ανήκει στα εσωτερικά πρωτόκολλα πυλών (Interior Gateway Protocol - IGP).
- Είναι πρωτόκολλο δρομολόγησης διανύσματος απόστασης (distance vector).
- Ως μέτρο για την επιλογή διαδρόμων χρησιμοποιείται ο αριθμός αλμάτων (hop count).
- Ο μέγιστος επιτρεπτός αριθμός αλμάτων είναι το 15.
- Οι ενημερώσεις δρομολόγησης με τη μορφή πίνακα δρομολόγησης εξ ορισμού εκπέμπονται κάθε 30 δευτερόλεπτα.
- Αναξιόπιστη μεταφορά μεταδόσεις μηνυμάτων μέσω UDP.
- Υποστηρίζει της διάδοσης προεπιλεγμένων διαδρομών.
- Μπορεί να εξισορροπήσει το φορτίο σε διαδρομές με το ίδιο κόστος.
- Το RIP-1 απαιτεί ότι για κάθε αριθμό κύριου δικτύου με κλάσεις που γνωστοποιείται μπορεί να χρησιμοποιηθεί μόνο μια μάσκα δικτύου. Η μάσκα αυτή είναι μια μάσκα υποδικτύου σταθερού μήκους.

- Το τυπικό RIP-1 δεν παρέχει ενεργοποιημένες ενημερώσεις (triggered updates) και χρησιμοποιεί εκπομπή μέσω υλικού (broadcast).
- Το RIP-2 επιτρέπει μάσκες υποδικτύου μεταβλητού μήκους (variable-length subnet mask - VLSM) και υποστηρίζει ενεργοποιημένες ενημερώσεις. Επίσης, επιτρέπει την επίδοση με πολυεκπομπή (multicast) και επικύρωση MD5.

9.4 Διαμόρφωση RIP

Στο παράδειγμα που παρουσιάζεται στο σχήμα 9-2, η αντιπυρική ζώνη ASA συνδέεται με ένα δρομολογητή που εκτελεί RIP-2. Αυτός ο δρομολογητής μαθαίνει τις διαδρομές από δύο άλλους δρομολογητές. Στη συνέχεια, οι διαδρομές από όλα αυτά τα δίκτυα διαφημίζονται από το δρομολογητή που συνδέεται με το ASA. Τέλος, η αντιπυρική ζώνη εγχέει (injecting) μια διαδρομή προεπιλογής στον εσωτερικό δρομολογητή.



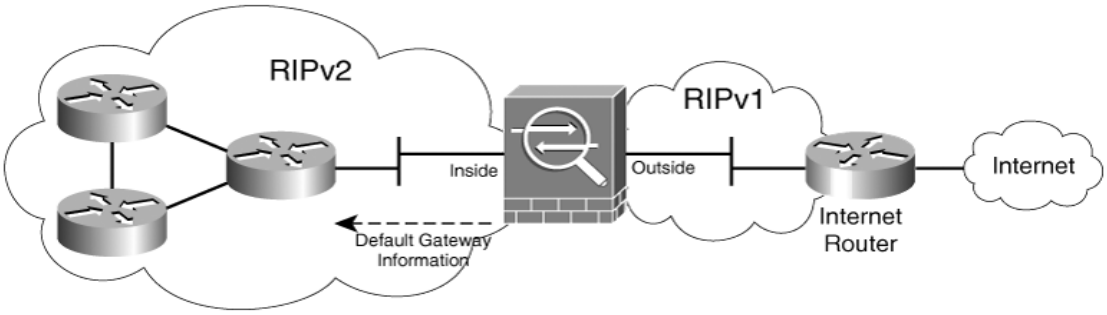
Σχήμα 9-2 : Βασική διαμόρφωση RIP

Το παράδειγμα 9.5 παρουσιάζει τις απαραίτητες εντολές για να διαμορφωθεί το RIPv2 και να διαφημίσει μια διαδρομή προεπιλογής στον εσωτερικό δρομολογητή. Η εντολή *rip* ενεργοποιεί και επιλεγεί ως πρωτόκολλο δρομολόγησης το RIP. Επίσης διευκρινίζεται η διεπαφή στην οποία θα επιτραπεί το RIP. Το επιθυμητό αποτέλεσμα είναι να γίνουν γνωστές οι εσωτερικές διαδρομές και να διαφημιστούν οι πληροφορίες για την διαδρομή προεπιλογής. Για αυτό το λόγο, χρησιμοποιείται η λέξη κλειδί *default*. Η λέξη κλειδί *default* διευκρινίζει την έκδοση RIP που χρησιμοποιείται. Με την λέξη

κλειδί passive, η διεπαφή παρακολουθεί τα πακέτα δρομολόγησης RIP και χρησιμοποιεί αυτές τις πληροφορίες για να ενημερώσει τον πίνακα δρομολόγησής, αλλά δεν διαφημίζει τις αναπροσαρμογές δρομολόγησης μέσω της συγκεκριμένης διεπαφής.

Παράδειγμα 9-5 : Βασική διαμόρφωση RIP
Fw1# configure terminal
Fw1(config)# rip inside passive version 2
Fw1(config)# rip inside default version 2

Μέσα από το παράδειγμα που παρουσιάζεται στο σχήμα 9-3 δείχνουμε πώς τα RIP-2 και RIP-1 μπορούν να διαμορφωθούν σε δύο διαφορετικές διεπαφές (inside και outside). Η εσωτερική διεπαφή διαμορφώνεται για RIP-2, όπως και στο προηγούμενο παράδειγμα. Επιπλέον, η αντιπυρική ζώνη ASA μαθαίνει τις διαδρομές RIP-1 στην εξωτερική διεπαφή του από το δρομολογητή Internet router. Οι εντολές που απαιτούνται για την παραπάνω διαμόρφωση παρουσιάζονται στο παράδειγμα 9-6.



Σχήμα 9-3: Διαμόρφωση RIP-1 και RIP-2 σε δύο διαφορετικές διεπαφές

Παράδειγμα 9-6 : Διαμόρφωση RIP-1 RIP-2 σε δύο διαφορετικές διεπαφές
Fw1# configure terminal
Fw1(config)# rip inside passive version 2
Fw1(config)# rip inside default version 2
Fw1(config)# rip outside passive version 1

Το RIP-1 δεν υποστηρίζει επικύρωση. Αντίθετα, το RIP-2 υποστηρίζει δύο τρόπους επικύρωσης: απλό κείμενο (plain-text) και Message Digest 5 (MD5). Η καλύτερη πρακτική είναι να χρησιμοποιηθεί MD5 αντί της επικύρωσης απλού κειμένου, επειδή η επικύρωση MD5 παρέχει ένα υψηλότερο επίπεδο ασφάλειας. Το παράδειγμα 6-3 παρουσιάζει τις απαραίτητες εντολές για ενεργοποίηση επικύρωσης μέσω MD5. Σε αυτό το παράδειγμα η λέξη *pass123* είναι ο κωδικός πρόσβασης MD5 και ο αριθμός 1 είναι η ταυτότητα προσδιορισμού επικύρωσης RIP-2. Αυτή η βασική ταυτότητα μπορεί να διαμορφωθεί με έναν αριθμό από 0 έως 255, αλλά πρέπει να ταιριάξει με τον αριθμό που είναι σε χρήση στον άλλο δρομολογητή.

Παράδειγμα 9-7 : Διαμόρφωση επικύρωσης RIP-2 MD5
Fw1(config)# rip inside default version 2 authentication md5 pass123 1

9.5 Έλεγχος διαμόρφωσης RIP

Η εντολή show route εμφανίζει τον πίνακα δρομολόγησης. Με αυτήν την εντολή, μπορούμε επίσης να ελέγχουμε ότι η συσκευή ασφάλειας είναι ενήμερη για τις σωστές δρομολογήσεις μέσω του RIP. Το παράδειγμα 9-8 παρουσιάζει την παραγωγή του πίνακα δρομολόγησης και τις δρομολογήσεις που έχουν αναγνωριστεί από άλλες συσκευές μέσω του RIP. Πριν από κάθε είσοδο δρομολόγησης υπάρχει ένα γράμμα. Το γράμμα R δείχνει ότι η διαδρομή μαθαίνεται μέσω RIP, ενώ το C ότι το αντίστοιχο δίκτυο είναι άμεσα συνδεδεμένο.

Παράδειγμα 9-8 : Εμφάνιση του πίνακα δρομολόγησης
Fw1# show route
R 0.0.0.0 0.0.0.0 [1/0] via 209.165.200.226, outside
C 192.168.10.0 255.255.255.0 is directly connected, inside
R 192.168.20.0 255.255.255.0 [1/0] via 192.168.10.2, inside
R 192.168.13.0 255.255.255.0 [2/0] via 192.168.10.2, inside
C 209.165.200.224 255.255.255.224 is directly connected, outside

9.6 Πρωτόκολλο προτεραιότητας ανοίγματος συντομότερης διαδρομής (OSPF)

Το πρωτόκολλο προτεραιότητας ανοίγματος συντομότερης διαδρομής (Open Shortest Path First - OSPF) αναπτύχθηκε για δίκτυα πρωτοκόλλου διαδικτύου (Internet Protocol - IP) από την ομάδα εργασίας του πρωτοκόλλου εσωτερικών πυλών (Interior Gateway Protocol - IGP) του ιδρύματος Internet Engineering Task Force (IETF). Αυτή η ομάδα σχηματιστικέ το 1988 για την σχεδίαση ενός IGP, με βάση το αλγόριθμο προτεραιότητας συντομότερης διαδρομής (Shortest Path First - SPF), ο όποιος μερικές φόρες αναφέρεται ως αλγόριθμος Dijkstra. Το OSPF είναι ένα ιεραρχικό πρωτόκολλο δρομολόγησης ανοιχτού προτύπου με βάση την κατάσταση της σύνδεσης (link-state). Η προδιαγραφή του πρωτόκολλου δημοσιεύεται ως έγγραφο RFC 1131 και η δεύτερη έκδοση περιγράφεται στο έγγραφο RFC 2328. Το πρωτόκολλο OSPF έχει τα παρακάτω χαρακτηριστικά:

- Δρομολόγηση μέσα σε ένα αυτόνομο σύστημα.
- Πλήρης υποστήριξη διευθυνσιοδότησης CIDR και υποδικτύου.
- Ανταλλαγή μηνυμάτων με πιστοποίηση ταυτότητας.
- Εισαγόμενα δρομολόγια.
- Αλγόριθμος κατάστασης συνδέσμων.
- Υποστήριξη για δίκτυα πολλαπλής πρόσβασης.

9.7 Κατηγορίες περιοχών και δρομολογητών στο OSPF

Ένα δίκτυο σύμφωνα με το OSPF διαχωρίζεται σε περιοχές. Αυτές οι περιοχές είναι λογικές ομάδες από δρομολογητές, των οποίων οι πληροφορίες συνοψίζονται και προωθούνται στο υπόλοιπο δίκτυο. Έχουν οριστεί αρκετές «ειδικές» περιοχές:

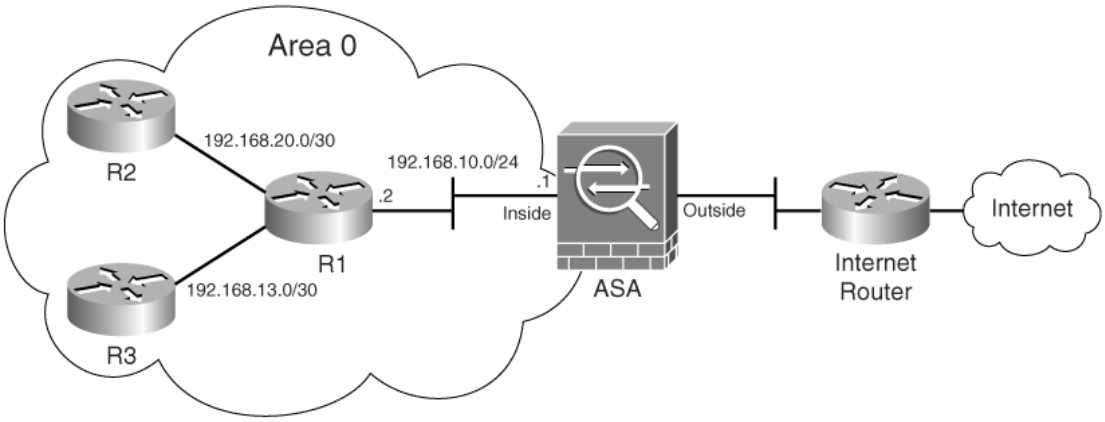
- **Περιοχή κορμού** (backbone area): Η περιοχή κορμού (επίσης γνωστή και ως περιοχή μηδέν) σχηματίζει τον πυρήνα ενός δικτύου που στηρίζεται στον OSPF. Όλες οι υπόλοιπες περιοχές συνδέονται σε αυτή, και η δια-περιοχιακή δρομολόγηση (inter-area routing) γίνεται μέσω ενός δρομολογητή που βρίσκεται στην περιοχή κορμού. Όλες οι περιοχές του OSPF θα πρέπει να συνδέονται με την περιοχή κορμού.
- **Περιοχή στελεχών** (Stub Area): Μια περιοχή στελεχών είναι μια περιοχή η οποία δεν λαμβάνει εξωτερικές διαδρομές (external routes). Οι εξωτερικές διαδρομές ορίζονται ως οι διαδρομές που διανέμονται στο OSPF από ένα άλλο πρωτόκολλο δρομολόγησης.
- **Πλήρως στελεχωμένη περιοχή** (Totally stubby area - TSA): Μια πλήρως στελεχωμένη περιοχή είναι παρόμοια με μια περιοχή στελεχών, ωστόσο αυτή η περιοχή δεν επιτρέπει διαδρομές συνοψισμού (summary routes) επιπρόσθετα στις εξωτερικές διαδρομές, αυτό σημαίνει, ότι δια-περιοχιακές διαδρομές δεν συνοψίζονται σε αυτές τις περιοχές. Ο μόνος τρόπος για να δρομολογηθεί η κίνηση έξω από την περιοχή είναι μια προεπιλεγμένη διαδρομή η οποία είναι και η μόνη Τύπου-3 LSA (Type-3 LSA) που διαφημίζεται στην περιοχή.
- **Όχι-τόσο-στελεχωμένη περιοχή** (Not-so-stubby area - NSSA) : Μια όχι-τόσο-στελεχωμένη περιοχή είναι ένας τύπος περιοχής στελεχών η οποία μπορεί να εισάγει διαδρομές από αυτόνομα συστήματα (Autonomous System - AS) και να τις στείλει στην περιοχή κορμού, αλλά δεν μπορεί να λάβει εξωτερικές διαδρομές από την περιοχή κορμού ή άλλες περιοχές.

Το OSPF ορίζει διάφορους τύπους δρομολογητών. Αυτοί η κατηγοριοποίηση είναι λογική και ένας δρομολογητής που χρησιμοποιεί το OSPF μπορεί να είναι ταξινομημένος σε περισσότερους από τους τύπους που ακολουθούν. Για παράδειγμα ένας δρομολογητής ο οποίος είναι συνδεδεμένος σε πάνω από μια περιοχές και λαμβάνει διαδρομές από μια διεργασία BGP που είναι συνδεδεμένη σε ένα άλλο αυτόνομο σύστημα είναι και ABR (Area Border Router) και ASBR (Autonomous System Boundary Router).

- **Δρομολογητής ορίων περιοχής** (Area Border Router - ABR): Ένας δρομολογητής ορίων περιοχής (ABR) είναι ένας δρομολογητής ο οποίος συνδέει μια η περισσότερες περιοχές OSPF στο κυρίως δίκτυο κορμού. Λειτουργεί σαν μέλος σε όλες τις περιοχές που είναι συνδεδεμένος. Ένας ABR κρατάει πολλαπλά αντίγραφα της βάσης δεδομένων κατάστασης συνδέσμων (link-state database) στην μνήμη, ένα για κάθε περιοχή.
- **Δρομολογητής ορίων αυτόνομου συστήματος** (Autonomous System Boundary Router - ASBR): Ένας δρομολογητής ορίων αυτόνομου συστήματος (ASBR) είναι ένας δρομολογητής ο οποίος είναι συνδεδεμένος περισσότερα από ένα AS και ανταλλάσσει πληροφορίες δρομολόγησης με δρομολογητές σε άλλα AS.
- **Εσωτερικός Δρομολογητής** (Internal Router - IR): Ένας δρομολογητής ονομάζεται εσωτερικός δρομολογητής (IR) αν έχει γείτονες μόνο δρομολογητές που ανήκουν στην ίδια περιοχή με αυτόν.
- **Δρομολογητής Κορμού** (Backbone Router - BR): Ένας δρομολογητής κορμού (BR) είναι ένας δρομολογητής, του οποίο μια διεπαφή είναι συνδεδεμένη με την περιοχή κορμού. Ένας ABR έιναι ένας BR, το αντίθετο μπορεί και να μην ισχύει.
- **Ορισμένος Δρομολογητές** (Designated Router - DR): Ένας ορισμένος δρομολογητής (DR) είναι ένας δρομολογητής ο οποίος εκλέγεται από το δίκτυο με εκλογές. Ένας DR εκλέγεται σύμφωνα με ορισμένα προεπιλεγμένα κριτήρια, οπός η προτεραιότητα και το RID (Router ID). Η προτεραιότητα παίρνει τιμές από 1 έως 255, όσο πιο μεγάλη η τιμή τόσο μεγαλύτερη η πιθανότητα να γίνει ένας δρομολογητής είτε DR είτε BDR.
- **Εφεδρικός Ορισμένος Δρομολογητής** (Backup Designated Router - BDR): Ένας εφεδρικός ορισμένος δρομολογητής (BDR) είναι ένας δρομολογητής ο οποίος γίνεται ορισμένος δρομολογητής αν ο υπάρχων ορισμένος δρομολογητής παρουσιάσει κάποια βλάβη. Ο BDR είναι ο OSPF δρομολογητής με την δεύτερη μεγαλύτερη προτεραιότητα.

9.8 Ενεργοποίηση OSPF

Η τοπολογία που δείχνει το σχήμα 9-4 περιλαμβάνει μια συσκευή ασφάλειας ASA με συνδεδεμένο στην εσωτερική διεπαφή τον δρομολογητή R1. Αυτός ο δρομολογητής συνδέεται επίσης με δύο άλλους δρομολογητές εσωτερικού δικτυού (τους R2 και R3).



Σχήμα 9-4 : Βασική διαμόρφωση OSPF

Σε αυτό το πρώτο παράδειγμα, τα ASA, R1, R2, και R3 διαμορφώνεται στην περιοχή 0. Για την αρχική διαμόρφωση του OSPF, θα πρέπει να εκτελεστούν τα παρακάτω βήματα:

Βήμα 1: Δημιουργία διαδικασίας δρομολόγησης OSPF. Ο αριθμός 1 χρησιμοποιείται ως παράμετρος προσδιορισμού για τη διαδικασία δρομολόγησης OSPF. Αυτός ο αριθμός δεν είναι απαραίτητο να ταιριάξει με τη διαδικασία των ομότιμων (peers) OSPF επειδή έχει μόνο τοπική σημασία. Μπορεί να διαμορφωθεί με μια τιμή από 1 έως 65,535 αλλά για κάθε διαδικασία δρομολόγησης OSPF θα πρέπει να διατεθεί μια μοναδική τιμή.

Παράδειγμα 9-9 : Διαδικασία δρομολόγησης OSPF
Fw1# configure terminal Fw1(config)# router ospf 1

Βήμα 2: Επιλογή διεπαφής στην οποία θα ενεργοποιηθεί το OSPF. Η εντολή *network* διευκρινίζει τις διεπαφές στις όποιες θα ενεργοποιηθεί το OSPF. Επιπλέον, διευκρινίζει την περιοχή που συνδέεται με εκείνη την διεπαφή, χρησιμοποιώντας τη διεύθυνση δικτύων ή τη διεύθυνση της διεπαφής όπου θέλουμε να επιτραπεί το OSPF. Στο παράδειγμα 9-10, η εντολή *network* προστίθεται στη διαμόρφωση και ακολουθείται από τη διεύθυνση δικτύων μάσκα των 24-bit. Η επιλογή *area 0* δείχνει ότι αυτή η διεπαφή έχει προστεθεί στην περιοχή 0. Ο ομότιμος OSPF θα πρέπει επίσης να διαμορφωθεί για την περιοχή 0.

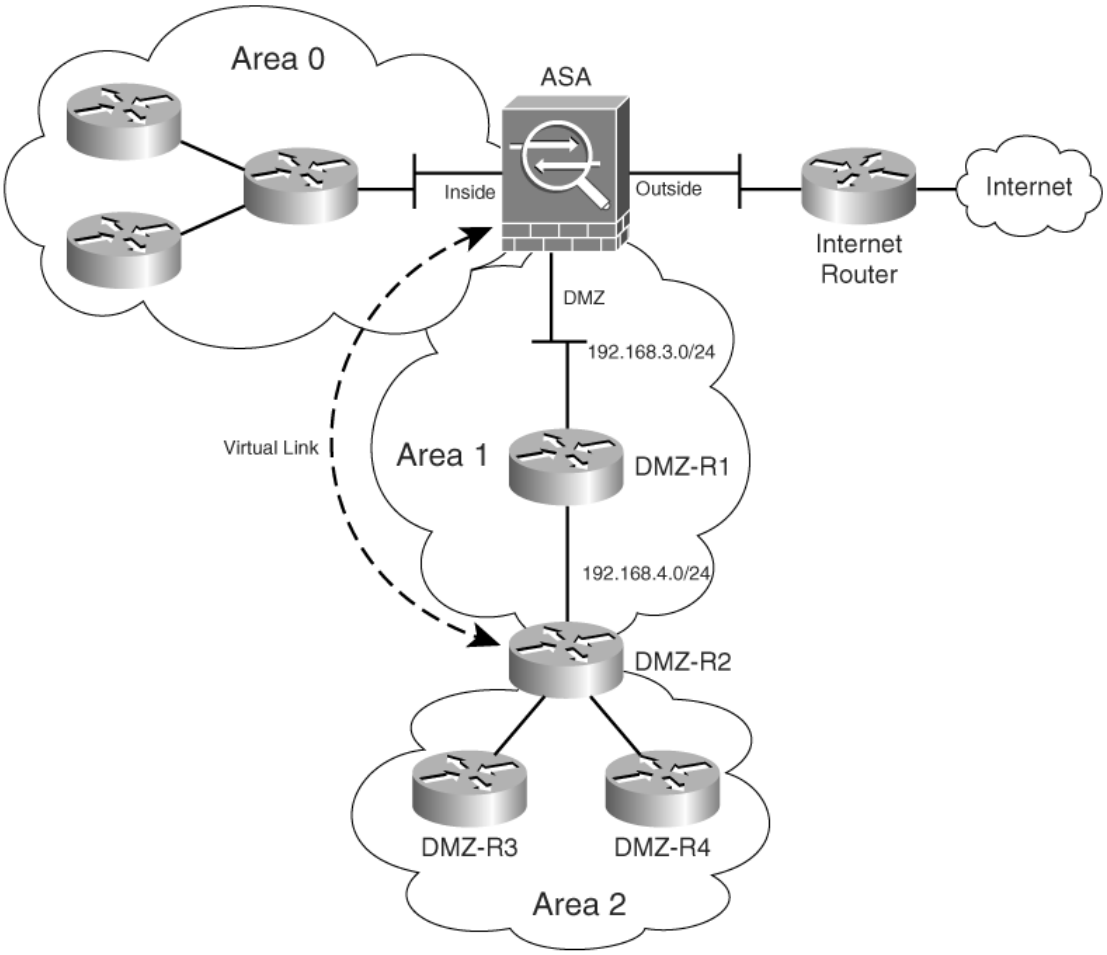
Παράδειγμα 9-10 : Ενεργοποίηση OSPF στην εσωτερική διεπαφή
Fw1# configure terminal
Fw1(config)# router ospf 1
Fw1(config-router)# network 192.168.10.0 255.255.255.0 area 0
Fw1(config-router)# exit

Στο παράδειγμα 9-11 εμφανίζεται ο πίνακας δρομολόγησης για την παραπάνω δρομολόγηση. Η έξοδος της εντολής *show route* δείχνει ότι στην εσωτερική διεπαφή υπάρχουν δύο διαδρομές που αναγνωρίζονται μέσω OSPF. Ο πρώτος αριθμός σε παρένθεση είναι η διοικητική απόσταση της πηγής πληροφοριών, ενώ ο δεύτερος αριθμός είναι το κόστος της διαδρομής.

Παράδειγμα 9-11 : Πίνακας δρομολόγησης
Fw1# show route
C 192.168.10.0 255.255.255.0 is directly connected, inside
C 209.165.200.224 255.255.255.224 is directly connected, outside
O 192.168.20.0 255.255.255.0 [110/11] via 192.168.10.2, 0:00:55, inside
O 192.168.13.0 255.255.255.0 [110/11] via 192.168.10.2, 0:00:55, Inside

9.9 Εικονικές συνδέσεις

Όλες οι περιοχές στο OSPF πρέπει να συνδέονται με την περιοχή μηδέν, αλλά σε πολλές περιπτώσεις αυτό δεν είναι εφικτό. Οι εικονικές συνδέσεις αποτελούν το μηχανισμό επίλυσης για αυτό πρόβλημα. Οι εικονικές συνδέσεις μπορούν να διαμορφωθούν για να συνδέσουν μια περιοχή μέσω μιας περιοχής που δεν αποτελεί περιοχή κορμού (nonbackbone). Το σχήμα 9-5 παρουσιάζει μια τοπολογία όπου μια συσκευή ασφάλειας ASA διαμορφώνεται για μια εικονική σύνδεση με το δρομολογητή που βρίσκεται στη διεπαφή DMZ.



Σχήμα 9-5 : Εικονικές συνδέσεις

Σε πρώτη φάση η εικονική σύνδεση δεν είναι ενεργή επειδή το ASA δεν γνωρίζει πώς να συνδεθεί με το δρομολογητή DMZ-R2. Προκειμένου το ASA να συνδεθεί επιτυχώς στο DMZ-R2 μέσω της περιοχής 1, πρέπει να διαδοθούν όλα τα LSA στην περιοχή 1 και να εκτελεστεί ο αλγόριθμος SPF. Σε αυτό το

παράδειγμα, η περιοχή 1 είναι περιοχή διέλευσης. Εφόσον το ASA επικοινωνήσει με το DMZ-R2, τότε θα προσπαθήσουν να διαμορφώσουν μια γειτνίαση (adjacency) μέσω της εικονικής σύνδεσης. Όταν αυτό επιτευχτεί, ο DMZ-R2 γίνεται ABR για την περιοχή, επειδή τώρα έχει και μια σύνδεση στην περιοχή 0. Συνεπώς, θα έχει δημιουργηθεί και ένα συνοπτικό LSA για τα δίκτυα στην περιοχή 0 και την περιοχή 1. Στο παράδειγμα 9-12 παρουσιάζει η εικονική διαμόρφωση συνδέσεων για το ASA. Η διεπαφή DMZ έχει διεύθυνση IP 192.168.4.1 και ο DMZ-R2 192.168.3.1.

Παράδειγμα 9-12 : Παράδειγμα διαμόρφωσης εικονικών συνδέσεων

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 209.165.200.225 255.255.255.248
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/2
nameif DMZ
security-level 50
ip address 192.168.4.1 255.255.255.0
!
router ospf 1
network 192.168.4.1 255.255.255.255 area 1
network 192.168.10.0 255.255.255.0 area 0
area 1 virtual-link 192.168.3.1
log-adj-changes
```

Στο παράδειγμα 9-13 παρουσιάζεται η έξοδος της εντολής *show ospf virtual-links* μετά την ενεργοποίηση της εικονικής σύνδεσης.

Παράδειγμα 9-13 : Αποτελέσματα εντολής show ospf virtual-links
Fw1# show ospf virtual-links
Virtual Link DMZ to router 192.168.3.1 is up
Run as demand circuit
DoNotAge LSA allowed.
Transit area 1, via interface DMZ, Cost of using 10
Transmit Delay is 1 sec, State UP,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit

ΚΕΦΑΛΑΙΟ 10
Intranet VPN

10.1 Εισαγωγή

Ιδεατό ιδιωτικό δίκτυο (Virtual Private Network) ονομάζεται η επέκταση του ιδιωτικού δικτύου ενός οργανισμού μέσω ενός δημόσιου δικτύου όπως το διαδίκτυο, δημιουργώντας μια ιδιωτική ασφαλή σύνδεση, χρησιμοποιώντας μια ιδιωτική σήραγγα. Τα VPN μπορούν να κάνουν ασφαλή μεταβίβαση πληροφοριών σε ολόκληρο το διαδίκτυο συνδέοντας τους μακρινούς χρήστες, επιμέρους υποκαταστήματα, και επιχειρησιακούς συνεργάτες σε ένα εκτεταμένο εταιρικό δίκτυο.

Σχήμα 10-3 : Ιδεατό ιδιωτικό δίκτυο

Αυτό το κεφάλαιο εστιάζει στη διαμόρφωση των Intranet Virtual Private Network (η αλλιώς site-to-site VPN), με βάση το πρωτόκολλο IP Security - IPSec, στις συσκευές ασφάλειας ASA και PIX. Παρουσιάζει έναν αρχικό πίνακα ελέγχου, τα βήματα της αντίστοιχης διαμόρφωσης και ένα ολοκληρωμένο σενάριο. Παρακάτω γίνεται μια ανάλυση της συντόμευσης VPN.

- **Είναι εικονικό:** Αυτό σημαίνει ότι η φυσική υποδομή του δικτύου πρέπει να είναι διαφανής σε οποιαδήποτε σύνδεση VPN. Στις περισσότερες περιπτώσεις το φυσικό δίκτυο δεν είναι το ιδιωτικό δίκτυο του χρήστη ενός VPN αλλά είναι ένα δημόσιο δίκτυο, μοιραζόμενο με πολλούς άλλους χρήστες. Για να διευκολυνθεί η απαραίτητη διαφάνεια προς τα ανώτερα στρώματα, χρησιμοποιούνται πρωτόκολλα που υποστηρίζουν τεχνική σήραγγας. Για να ξεπεραστούν οι επιπτώσεις της

μη ιδιοκτησίας του φυσικού δικτύου, γίνονται συμφωνίες παροχής υπηρεσιών με τους προμηθευτές δικτύων (network providers) για να παρέχουν, με τον καλύτερο δυνατό τρόπο, τις απαιτήσεις απόδοσης και διαθεσιμότητας που είναι αναγκαίες σε ένα VPN.

- **Είναι ιδιωτικό:** Ο όρος "ιδιωτικός" στα πλαίσια ενός VPN αναφέρεται στη μυστικότητα της ροής δεδομένων πάνω από το VPN. Τα δεδομένα σε ένα VPN συχνά περνούν πάνω από δημόσια δίκτυα και επομένως, πρέπει να υπάρχει πρόνοια ώστε να τηρηθούν συγκεκριμένες απαιτήσεις ασφάλειας

- **Είναι δίκτυο:** Ακόμη κι αν όχι φυσικά υπαρκτό, ένα VPN πρέπει να γίνει αντιληπτό και να αντιμετωπίζεται ως επέκταση της υποδομής δικτύων μιας επιχείρησης. Αυτό σημαίνει ότι πρέπει είναι διαθέσιμο και στο υπόλοιπο του δικτύου, σε όλο η σε ένα υποσύνολο των συσκευών και των εφαρμογών, επηρεάζοντας διευθυνσιοδότηση και δρομολόγηση.

10.2 Αρχικός έλεγχος

Το IPSec μπορεί να χρησιμοποιήσει το πρωτόκολλο IKE (Internet Key Exchange) για τη βασική διαχείριση και διαπραγμάτευση των σηράγγων επικοινωνίας. Το IKE χρησιμοποιεί έναν συνδυασμό από ιδιότητες της φάσης 1 και φάσης 2 για τη διαπραγμάτευση μεταξύ των ομότιμων. Εάν δεν έχει διαμορφωθεί σωστά οποιαδήποτε από τις ιδιότητες, τότε η σήραγγα IPSec θα αποτύχει να καθιερωθεί. Επομένως είναι ιδιαίτερα σημαντική η σημασία της κατανόησης ενός πίνακα ελέγχου πριν την διαμόρφωση. Ο πίνακας 10-1 απαριθμεί όλες τις πιθανές τιμές που υποστηρίζονται από της συσκευές ασφάλειας ASA και PIX για τις ιδιότητες της πρώτης φάσης. Περιλαμβάνει επίσης τις προκαθορισμένες τιμές για κάθε ιδιότητα. Θα πρέπει επιπρόσθετα να δοθεί έμφαση στις επιλογές και τις παραμέτρους που θα διαμορφωθούν στο άλλο άκρο της σήραγγας VPN.

Πίνακας 10-1 : Ιδιότητες ISAKMP		
Ιδιότητες	*Πιθανές τιμές*	*Προκαθορισμένη τιμή*
Κρυπτογράφηση	DES 56-bit 3DES 168-bit AES 128-bit AES 192-bit AES 256-bit	3DES 168-bit ή DES 56-bit
Συνάρτηση Hash	MD5 ή SHA	SHA
Μέθοδος επικύρωσης	Κλειδιά Preshared Υπογραφή RSA Υπογραφή DSA	Κλειδιά Preshared
Ομάδα DH	Group 1 768-bit Group 2 1024-bit Group 5 1536-bit Group 7 ECC 163-bit	Group 2 1024-bit
Διάρκεια ζωής	120–2,147,483,647 δευτερόλεπτα	86.400 δευτερόλεπτα

Εκτός από τις παραμέτρους IKE, οι δύο συσκευές IPSec διαπραγματεύονται και τον τρόπο λειτουργίας. Το ASA χρησιμοποιεί τον κύριο τρόπο (main mode) ως μέθοδο προεπιλογής για τις ιντρανέτ σήραγγες αλλά επίσης μπορεί να χρησιμοποιήσει και τον επιθετικό τρόπο (aggressive mode). Μετά την διαπραγμάτευση των ιδιοτήτων της πρώτης φάσης, είναι σημαντικό να δοθεί έμφαση στις ιδιότητες της δεύτερης φάσης της σύνδεση VPN. Οι συσχετίσεις ασφάλειας (security associations - SA) της δεύτερης φάσης χρησιμοποιούνται για την κρυπτογράφηση και αποκρυπτογράφηση της πραγματικής κυκλοφορίας δεδομένων. Οι συγκεκριμένες συσχετίσεις ασφάλειας αναφέρονται επίσης ως IPSec SAs. Ο πίνακας 10-2 απαριθμεί τις ιδιότητες που υποστηρίζονται από της συσκευές ασφάλειας ASA και PIX, για την δεύτερη φάση και τις αντίστοιχες προκαθορισμένες τιμές.

Πίνακας 10-2 : Ιδιότητες IPSec		
Ιδιότητες	*Πιθανές τιμές*	*Προκαθορισμένες τιμές*
Κρυπτογράφηση	Όχι DES 56-bit 3DES 168-bit AES 128-bit AES 192-bit AES 256-bit	3DES 168-bit ή DES 56-bit
Συνάρτηση Hash	MD5, SHA ή Όχι	Όχι
Πληροφορίες ταυτότητας	Πρωτόκολλο - αριθμός θύρας	Καμία παράμετρος προεπιλογής
Διάρκεια ζωής	120-2,147,483,647 δευτερόλεπτα 10-2,147,483,647 KB	28800 δευτερόλεπτα 4,608,000 KB
Τρόπος	Σήραγγα ή μεταφορά	Σήραγγα
Ομάδα PFS	Όχι Group 1 768-bit DH Group 2 1024-bit DH Group 5 1536-bit DH Group 7 ECC 163-bit	Όχι

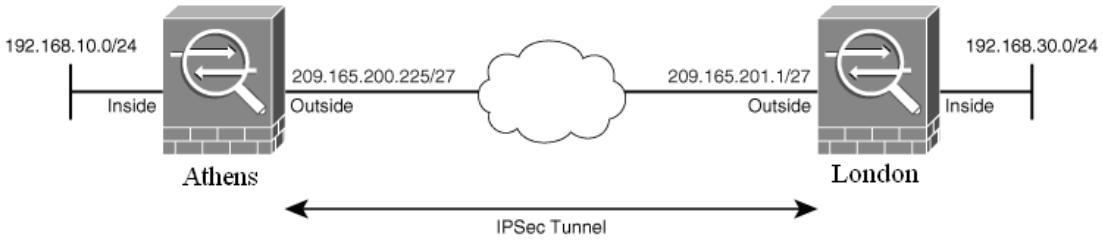
10.3 Βήματα διαμόρφωσης

Η διαμόρφωση σήραγγας για ένα ιντρανέτ IPSec VPN χωρίζεται σε 10 βήματα:

- Βήμα 1. Ενεργοποίηση ISAKMP.
- Βήμα 2. Δημιουργία πολιτικής ISAKMP.
- Βήμα 3. Επιλογή τύπου σήραγγας.
- Βήμα 4. Διαμόρφωση κλειδιών.

- Βήμα 5. Επιλογή πολιτικής IPSec.
- Βήμα 6. Ορισμός ενδιαφέρουσας κυκλοφορίας.
- Βήμα 7. Διαμόρφωση χάρτη κρυπτογράφησης.
- Βήμα 8. Εφαρμογή χάρτη κρυπτογράφησης στη διεπαφή.
- Βήμα 9. Διαμόρφωση φιλτραρίσματος κυκλοφορίας.
- Βήμα 10. Παράκαμψη NAT. (προαιρετικό)

Το σχήμα 10-2 παρουσιάζει μια τοπολογία ενός υποθετικού οργανισμού με δυο κεντρικές τοποθεσίες σε Αθήνα και Λονδίνο. Για την υλοποίηση των παραπάνω βημάτων και την διαμόρφωση του VPN θα χρησιμοποιηθεί η συσκευή ασφάλειας που έχει τοποθετηθεί στην Αθήνα.



Σχήμα 10-2 : Τοπολογία δικτυού VPN

Βήμα 1. Ενεργοποίηση ISAKMP: Η διαμόρφωση της πρώτης φάσης του IKE αρχίζει με την ενεργοποίηση του ISAKMP στη διεπαφή που θα τερματίζει τις σήραγγες VPN. Συνήθως, γίνετε στην εξωτερική διεπαφή που αποτελεί και την σύνδεση με το διαδίκτυο. Το παράδειγμα 10-1 παρουσιάζει την ενεργοποίηση του ISAKMP στην εξωτερική διεπαφή.

Παράδειγμα 10-1 : Ενεργοποίηση ISAKMP στην εξωτερική διεπαφή
Athens# configure terminal Athens(config)# isakmp enable outside

Βήμα 2. Δημιουργία πολιτικής ISAKMP: Μετά την ενεργοποίηση του ISAKMP στη διεπαφή, το επόμενο βήμα είναι η δημιουργία μιας πολιτικής για την πρώτη φάση. Η συγκεκριμένη πολίτικη θα πρέπει να ταιριάζει με το άλλο άκρο της σύνδεσης VPN. Αυτή η εργασία ολοκληρώνετε μέσω της εντολής

isakmp policy. Σε περίπτωση που έχουν διαμορφωθεί περισσότερο από μια πολιτικές ISAKMP, τότε επιλέγετε η πολιτική με την πιο υψηλή προτεραιότητα. Εάν δεν υπάρξει καμία αντιστοιχία, ελέγχετε η πολιτική με την επόμενη πιο υψηλή προτεραιότητα και αυτό συνεχίζεται μέχρι το σημείο που θα έχουν αξιολογηθεί όλες οι πολιτικές. Μια τιμή προτεραιότητας που θα ισούται με ένα θα είναι και η πιο υψηλή προτεραιότητα, ενώ μια τιμή προτεραιότητας 65535 θα είναι η χαμηλότερη. Εάν κάποια από τις ιδιότητες ISAKMP δεν έχει διαμορφωθεί, τότε η ασφάλεια προσθέτει στις ιδιότητες την προκαθορισμένη τιμή. Το παράδειγμα 10-2 παρουσιάζει μια πολιτική ISAKMP με κρυπτογράφηση AES-256, MD5 hash, ομάδα DH 5 και επικύρωση κλειδιών με διάρκεια ζωής 28.800 δευτερόλεπτα.

Παράδειγμα 10-2 : Δημιουργία πολιτικής ISAKMP
Athens# configure terminal
Athens(config)# isakmp policy 10 authentication pre-share
Athens(config)# isakmp policy 10 encryption aes-256
Athens(config)# isakmp policy 10 hash md5
Athens(config)# isakmp policy 10 group 5
Athens(config)# isakmp policy 10 lifetime 28800

Βήμα 3. Επιλογή τύπου σήραγγας: Μια σήραγγα IPSec μπορεί να διαμορφωθεί για δυο διαφορετικούς τύπους σύνδεσης:

- Απομακρυσμένη πρόσβαση (remote access)
- Περιοχή με περιοχή (site to site)

Στην δεύτερη περίπτωση, ο τύπος της σήραγγας ορίζεται σε *ipsec-l2l*, ενώ το όνομα του πεδίου *tunnel-group* είναι η διεύθυνση IP του ομότιμου. Η εντολή tunnel group δημιουργεί και διαχειρίζεται τη βάση δεδομένων των στατικών σηράγγων και για τους δυο τύπους σύνδεσης. Το παράδειγμα 10-3 επεξηγεί πώς μπορεί να διαμορφωθεί μια σήραγγα μεταξύ δυο δικτύων εάν η διεύθυνση IP στο απέναντι άκρο είναι 209.165.201.1.

Παράδειγμα 10-3 : Επιλογή τύπου σήραγγας
Athens(config)# tunnel-group 209.165.201.1 type ipsec-l2l

Βήμα 4. Διαμόρφωση κλειδιών ISAKMP: Εάν η πολιτική ISAKMP χρησιμοποιήσει τα προ-μοιρασμένα κλειδιά ως μέθοδο επικύρωσης, τότε ένα προ-μοιρασμένο κλειδί θα πρέπει να διαμορφωθεί κάτω από το δευτερεύον μενού *ipsec-attributes* της εντολής *tunnel-group*. Η σύνταξη της εντολής για την σύνδεση των ιδιοτήτων τιυ IPSec με ένα ομότιμο είναι της μορφής: tunnel-group *tunnel-group-name* ipsec-attributes. Η εκτέλεση της παραπάνω εντολής μας οδηγεί σε ένα δευτερεύον μενού, όπου μπορούμε να ορίσουμε το προ-μοιρασμένο κλειδί κρυπτογράφησης. Όπως φαίνεται και στο παράδειγμα 10-4, το ASA διαμορφώνεται με το κλειδί pass123 και διεύθυνση IP για τον ομότιμο 209.165.201.1.

Παράδειγμα 10-4 : Διαμόρφωση προ-μοιρασμένου κλειδιού
Athens(config)# tunnel-group 209.165.201.1 ipsec-attributes Athens(config-ipsec)# pre-shared-key pass123

Βήμα 5. Επιλογή πολιτικής IPSec: Το σύνολο μετατροπής (transform set) IPSec καθορίζει τον τύπο κρυπτογράφησης και την συνάρτηση hash που θα εφαρμοστεί στα πακέτα δεδομένων μετά την ενεργοποίηση της σήραγγας. Το σύνολο μετατροπής IPSec διαπραγματεύεται κατά τη διάρκεια της ταχείας μεθόδου (quick mode). Για να διαμορφωθεί το σύνολο μετατροπής, χρησιμοποιείτε η ακόλουθη σύνταξη:

crypto ipsec transform-set *transform-set-name* {esp-3des | esp-aes | esp-aes-192 | esp- aes-256 | esp-des | esp-md5-hmac | esp-null | esp-sha-hmac}

Εάν μια πολιτική IPSec διαμορφώνεται με ένα σύνολο μετατροπής που χρησιμοποίει αλγόριθμο κρυπτογράφησης όπως το esp-aes, η συσκευή ασφάλειας προσθέτει προκαθορισμένη επιλογή για hashing το esp-none. Επιπλέον, εάν το hashing διαμορφώνεται χωρίς αλγόριθμο κρυπτογράφησης, η συσκευή ασφάλειας προσθέτει ως αλγόριθμο κρυπτογράφησης προεπιλογής esp-3des. Το παράδειγμα 10-5 δείχνει μια διαμόρφωση με κρυπτογράφηση για τα πακέτα δεδομένων AES-256 και hashing SHA. Το όνομα του συνόλου μετατροπής ορίζεται σε myset.

Παράδειγμα 10-5 : Διαμόρφωση του συνόλου μετατροπής
Athens(config)# crypto ipsec transform-set myset esp-aes-256 esp-sha-hmac

Βήμα 6. Ορισμός ενδιαφέρουσας κυκλοφορίας : Για να καθορίσει την κυκλοφορία που πρέπει να κρυπτογραφηθεί, η συσκευή ασφάλειας χρησιμοποιεί μια λίστα ελέγχου πρόσβασης. Για κάθε εισερχόμενο πακέτο λαμβάνεται μια απόφαση δρομολόγησης με βάση την διεύθυνση προορισμού IP. Όταν το πακέτο εξέρχεται από μια διεπαφή που έχει διαμορφωθεί για μια σήραγγα VPN, ελέγχεται από το μηχανισμό κρυπτογράφησης για το αν συμπίπτει στις crypto καταχωρήσεις ελέγχου πρόσβασης (ACE). Εάν βρεθεί κάποια αντιστοιχία, το πακέτο κρυπτογραφείται και στη συνεχεία στέλνεται στον ομότιμο VPN. Μια ACL μπορεί να είναι απλή και να επιτρέπει όλη την IP κυκλοφορία μεταξύ των δικτύων ή περίπλοκη, ώστε να επιτρέπει μόνο την κυκλοφορία που προέρχεται από μια συγκεκριμένη IP διεύθυνση και θύρα πηγής και προορίζεται σε μια συγκεκριμένη IP διεύθυνση και θύρα προορισμού.

Οι κατάλογοι πρόσβασης εκτελούν επίσης και έλεγχο ασφάλειας για την εισερχόμενη κρυπτογραφημένη κυκλοφορία. Εάν ένα πακέτο δεν ταιριάζει με κάποιο crypto ACE, τότε η συσκευή ασφάλειας θα το απορρίψει και θα παράγει ένα μήνυμα syslog που θα εμφανίζει αυτό το γεγονός. Όπως φαίνεται και στο παράδειγμα 10-6, το Athens ASA διαμορφώνεται για να προστατεύσει όλη την κυκλοφορία IP που προέρχεται από το δίκτυο 192.168.10.0 με μάσκα 255.255.255.0 και προορίζεται στο δίκτυο 192.168.30.0 με μάσκα 255.255.255.0. Το όνομα της ACL είναι encrypt-acl.

Παράδειγμα 10-6 : ACL κρυπτογράφησης
Athens(config)# access-list encrypt-acl extended permit ip 192.168.10.0 255.255.255.0 192.168.30.0 255.255.255.0

Η συσκευή ασφάλειας ASA δεν επιτρέπει την πρόσβαση στην εσωτερική διεπαφή εάν η κυκλοφορία έρχεται από μια σήραγγα VPN. Αυτό ισχύει ακόμα και αν το εσωτερικό δίκτυο συμπεριλαμβάνεται στην ACL κρυπτογράφησης. Η διαχείριση της εσωτερικής διεπαφής για την κυκλοφορία VPN μπορεί να

επιτραπεί με τη χρησιμοποίηση της εντολής *management-access* ακολουθουμένη από το όνομα της διεπαφής. Στο παράδειγμα 10-7, η εσωτερική διεπαφή διαμορφώνεται ώστε να επιτρέπεται η πρόσβαση διαχείρισης.

Παράδειγμα 10-7 : Πρόσβαση διαχείρισης στην εσωτερική διεπαφή
Athens(config)# management-access inside

Βήμα 7. Διαμόρφωση χάρτη κρυπτογράφησης: Μετά την διαμόρφωση της πολίτικης για την πρώτη και δεύτερη φάση, το επόμενο βήμα είναι να δημιουργηθεί ένας χάρτης κρυπτογράφησης (crypto map) που θα χρησιμοποιήσει αυτές τις πολιτικές. Ένας χάρτης κρυπτογράφησης θεωρείται πλήρης όταν έχει τις ακόλουθες παραμέτρους:

- Τουλάχιστον ένα σύνολο μετατροπής
- Τουλάχιστον έναν ομότιμο VPN
- Μια crypto ACL

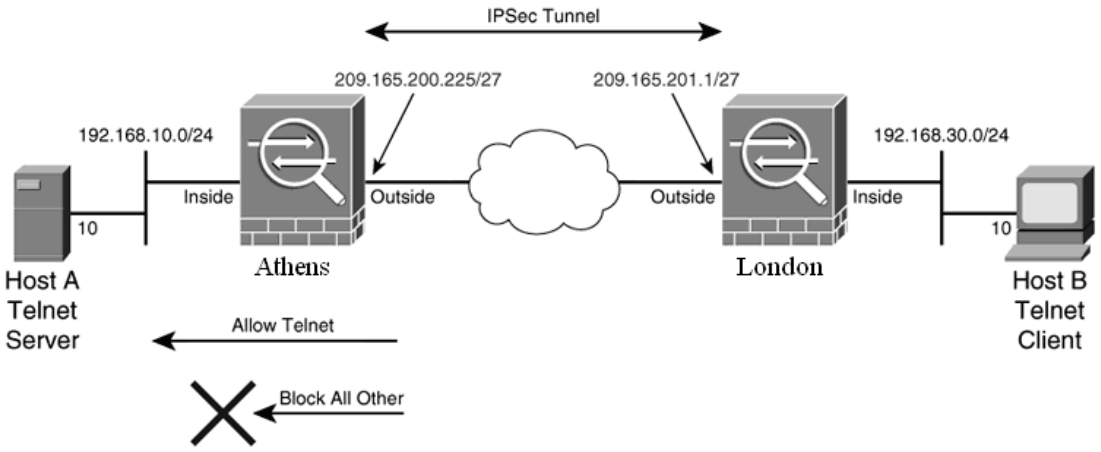
Το παράδειγμα 10-8 παρουσιάζει την διαμόρφωση του χάρτη κρυπτογράφησης στο Athens ASA. Το όνομα του crypto map είναι IPsec_map και ο αριθμός ακολουθίας που χρησιμοποιείται είναι 10. Ο αριθμός ακολουθίας χρησιμοποιείται για να καθορίσει πολλαπλάσιες σήραγγες IPSec που προορίζονται σε διαφορετικούς ομότιμους. Εάν η συσκευή ασφάλειας τερματίζει μια σήραγγα IPSec από έναν άλλο ομότιμο VPN, η δεύτερη σήραγγα VPN μπορεί να καθοριστεί χρησιμοποιώντας το υπάρχον όνομα του crypto map με έναν διαφορετικό αριθμό ακολουθίας. Κάθε αριθμός ακολουθίας προσδιορίζει μοναδικά μια σήραγγα VPN. Ωστόσο, η συσκευή ασφάλειας αξιολογεί πρώτα τη σήραγγα με το χαμηλότερο αριθμό ακολουθίας.

Παράδειγμα 10-8 : Διαμόρφωση του crypto map
Athens(config)# crypto map IPsec_map 10 set peer 209.165.201.1 Athens(config)# crypto map IPsec_map 10 set transform-set myset Athens(config)# crypto map IPsec_map 10 match address encrypt-acl

Βήμα 8. Εφαρμογή χάρτη κρυπτογράφησης στη διεπαφή: Μετά την διαμόρφωση ένας χάρτη κρυπτογράφησης, το τελικό βήμα είναι να συνδεθεί με μια διεπαφή. Συνήθως, εφαρμόζεται στη διεπαφή που είναι συνδεδεμένη με το διαδίκτυο και τερματίζει τις συνδέσεις VPN. Το παράδειγμα 10-9 επιδεικνύει πώς ένα crypto map με όνομα *IPsec_map* εφαρμόζεται στην εξωτερική διεπαφή.

Παράδειγμα 10-9 : Εφαρμογή crypto map εξωτερική διεπαφή
Athens# configure terminal Athens(config)# crypto map IPsec_map interface outside

Βήμα 9. Διαμόρφωση φιλτραρίσματος κυκλοφορίας: Όπως και μια παραδοσιακή αντιπυρική ζώνη, η συσκευή ασφάλειας ASA προστατεύει το εσωτερικό δίκτυο από την εξωτερική κυκλοφορία. Για να εισέρθει τέτοια κυκλοφορία, θα πρέπει πρώτα να έχει επιτραπεί ρητά από κάποια ACL. Η ίδια λογική εφαρμόζεται και όταν αποκρυπτογραφούνται τα πακέτα από τη μηχανή IPSec. Εάν δεν υπάρχει καμία άδεια στον εξωτερικό κατάλογο πρόσβασης διεπαφών, η συσκευή ασφάλειας απορρίπτει τα αποκρυπτογραφημένα πακέτα. Στο σχήμα 10-3, στο Host B επιτρέπεται να στείλει κυκλοφορία μόνο στο Host A, που βρίσκεται στην άλλη άκρη σήραγγα VPN, στη TCP θύρα 23. Στο παράδειγμα 10-10 το Athens ASA χρησιμοποίει στην εξωτερική διεπαφή την εισερχόμενη λίστα έλεγχου πρόσβασης *outside_acl*.



Σχήμα 10-3 : Φιλτράρισμα κυκλοφορίας VPN

Παράδειγμα 10-10 : Φιλτράρισμα κυκλοφορίας VPN
Athens(config)# access-list outside_acl extended permit tcp host 192.168.30.10 host 192.168.10.10 eq 23 Athens(config)# access-group outside_acl in interface outside

Στα περισσότερα σενάρια VPN, το απομακρυσμένο ιδιωτικό δίκτυο θεωρείται πλήρως εμπιστευόμενο και η δημιουργία πολλαπλάσιων καταχωρήσεων στις ACL των εξωτερικών διεπαφών, για να επιτραπεί η αποκρυπτογραφημένη κυκλοφορία IPSec, μπορεί να οδηγήσει σε ένα δύσχρηστο μοντέλο. Για την διευκόλυνση της διαμόρφωσης, το ASA υποστηρίζει την διαμόρφωση ενός IPSec sysopt. Αυτό επιτρέπει σε όλα τα αποκρυπτογραφημένα πακέτα IPSec να περάσουν μέσα από την συσκευή ασφάλειας χωρίς επιθεώρηση ενάντια στις ACL διεπαφών. Στο παράδειγμα 10-11 μετά την διαμόρφωση του IPSec sysopt το Athens ASA θα επιτρέπει όλη την αποκρυπτογραφημένη κυκλοφορία. Η εντολή *sysopt connection permit-ipsec* είναι μια σφαιρική εντολή και εάν ενεργοποιηθεί η ασφάλεια ασφάλειας θα παρακάμπτει τον έλεγχο των ACL για όλες τις σήραγγες IPSec.

Παράδειγμα 10-11 : Παράκαμψη φιλτραρίσματος κυκλοφορίας
Athens(config)# sysopt connection permit-ipsec

Βήμα 10. Παράκαμψη NAT: Στις περισσότερες περιπτώσεις, δεν θέλουμε να αλλάξουμε τις διευθύνσεις IP για την κυκλοφορία που περνά μέσα από μια σήραγγα. Εάν ενεργοποιηθεί το NAT η συσκευή ασφάλειας ASA θα αλλάξει τις διευθύνσεις IP. Για να παρακαμφθεί η μετάφραση των διευθύνσεων θα χρειαστεί να διαμορφωθούν κανόνες απαλλαγής.. Στο παράδειγμα 10-12 διαμορφώνεται μια ACL, με το όνομα *nonat*, για να διευκρινίσει την κυκλοφορία που πρέπει να παρακαμφθεί από την μηχανή NAT. Τα δίκτυα που θα περιλαμβάνει η ACL είναι από 192.168.10.0/24 έως 192.168.30.0/24.

Παράδειγμα 10-12 : ACL για να παρακαμφθεί το NAT
Athens(config)# access-list nonat extended permit ip 192.168.10.0 255.255.255.0 192.168.30.0 255.255.255.0

Μετά τον προσδιορισμό της ACL, το επόμενο βήμα είναι να διαμορφωθεί η εντολή *nat 0*. Στο παράδειγμα 10-13 δίνεται ο τρόπος διαμόρφωσης της δήλωση nat 0, όταν το προστατευμένο ιδιωτικό τοπικό LAN ανήκει στην εσωτερική διεπαφή.

Παράδειγμα 10-13 : ACL για να παρακαμφθεί το NAT
Athens(config)# nat (inside) 0 access-list nonat

10.4 Ολοκληρωμένη διαμόρφωση

Το παράδειγμα 10-14 παρουσιάζει μια πλήρη διαμόρφωση του Athens ASA για ένα site-to-site IPSec VPN, και ομότιμο 209.165.201.1. Η μόνη διάφορα στο προγραμματισμό του London ASA είναι οι διευθύνσεις των δικτύων.

Παράδειγμα 10-14 : Ολοκληρωμένη διαμόρφωση IPSec VPN
!
access-list encrypt-acl extended permit ip 192.168.10.0 255.255.255.0 192.168.30.0 255.255.255.0
access-list nonat extended permit ip 192.168.10.0 255.255.255.0 192.168.30.0 255.255.255.0
!
nat (inside) 0 access-list nonat
!
crypto ipsec transform-set myset esp-aes-256 esp-sha-hmac
!
crypto map IPSec_map 10 match address encrypt-acl
crypto map IPSec_map 10 set peer 209.165.201.1
crypto map IPSec_map 10 set transform-set myset
crypto map IPSec_map interface outside
!
isakmp enable outside
!

```
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 28800
!
tunnel-group 209.165.201.1 type ipsec-l2l
tunnel-group 209.165.201.1 ipsec-attributes
pre-shared-key pass123
sysopt connection permit-ipsec
!
```

10.5 Έλεγχος και ανίχνευσης λαθών στα IPSec VPN

Εάν χρειαστεί να γίνει έλεγχος της κατάστασης των σηράγγων IPSec, το αρχικό βήμα είναι η εξέταση της κατάστασης για την πρώτη φάση SA. Η εκτέλεση της εντολής *show crypto isakmp sa detail*, παρουσιάζεται στο παράδειγμα 10-15. Εάν οι διαπραγματεύσεις ISAKMP είναι επιτυχείς, τότε η κατάσταση θα είναι της μορφής *MM_ACTIVE*. Επίσης, η έξοδος της εντολής εμφανίζει τον τύπο της σήραγγας IPSec.

Παράδειγμα 10-15 : Έλεγχος πρώτης φάσης

```
Athens# show crypto isakmp sa detail
  Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
1   IKE Peer: 209.165.201.1
   Type    : L2L             Role    : responder
   Rekey   : no              State   : MM_ACTIVE
   Encrypt : aes-256         Hash    : MD5
   Auth    : preshared       Lifetime: 86400
   Lifetime Remaining: 36536
```

Εάν για κάποιο λόγο η σήραγγα IPSec δεν λειτουργεί σωστά. τότε θα πρέπει να ενεργοποιηθεί το αντιστοιχώ debug. Στο παράδειγμα 10-16 παρουσιάζονται οι δυο πιο σημαντικές εντολές για debug.

Παράδειγμα 10-16 : Έλεγχος πρώτης φάσης
debug crypto isakmp [debug level 1-255] debug crypto ipsec [debug level 1-255]

Εξ ορισμού, το επίπεδο έλεγχο είναι ένα και μπορεί να αυξηθεί μέχρι το 255 για ακόμα πιο λεπτομερή έξοδο. Ωστόσο, στις περισσότερες περιπτώσεις, ένα επίπεδο του logging με τιμή 127 δίνει αρκετές πληροφορίες για να ανακαλυφθεί η πρωταρχική αιτία του προβλήματος.

ΚΕΦΑΛΑΙΟ 11
Συμπεράσματα

Από την παραπάνω διπλωματική εργασία καταλήξαμε σε συμπεράσματα, τόσο θεωρητικού όσο και πρακτικού ενδιαφέροντος, σχετικά με τον σχεδιασμό και την διαμόρφωση των αντιπυρικών ζωνών στα σημερινά δίκτυα.

Όσο αφορά το θεωρητικό κομμάτι, έγινε αντιληπτό ότι οι αντιπυρικές ζώνες, ανεξάρτητα από την πολυπλοκότητα του σχεδιασμού και της υλοποίησης, έχουν την ευθύνη να ενεργήσουν ως σημεία επιβολής της πολιτικής ασφάλειας. Αυτό επιτυγχάνεται με την επιθεώρηση των δεδομένων που λαμβάνονται και την παρακολούθηση των συνδέσεων, ώστε να καθοριστούν τα δεδομένα που πρέπει να επιτραπούν η όχι. Επιπλέον, οι αντιπυρικές ζώνες μπορούν να ενεργήσουν ως ενδιάμεσοι και πληρεξούσιοι στα αιτήματα ενός προστατευμένου συστήματος, παρέχοντας συγχρόνως επικύρωση πρόσβασης για να εξασφαλίσουν ότι χορηγείται μόνο εγκεκριμένη πρόσβαση. Τέλος, οι αντιπυρικές ζώνες μπορούν να υποβάλουν εκθέσεις και προειδοποιήσεις σχετικά με τα γεγονότα και τις διαδικασίες, επιτρέποντας στον διαχειριστή να γνωρίζει την κατάσταση της αντιπυρικής ζώνης και των συστημάτων που προστατεύει.

Η σημαντικότερη εργασία που μπορεί να γίνει για να εξασφαλιστεί ότι μια αντιπυρική ζώνη μπορεί να προστατεύσει αποτελεσματικά τους πόρους, γίνεται με τη λήψη της καλύτερης απόφασης σχετικά με το τι πρέπει να προστατεύσει και πού θα τοποθετηθεί. Είναι σημαντικό να γίνει κατανοητός ο σχεδιασμός αντιπυρικών ζωνών που θα προστατεύσει καλύτερα τους πόρους που χρειάζονται προστασία. Αν και μια αντιπυρική ζώνη θα δίνει μια επαρκή προστασία των περισσότερων πόρων, ορισμένα περιβάλλοντα υψηλής ασφάλειας μπορούν να χρησιμοποιήσουν μια αρχιτεκτονική διπλών-αντιπυρικών ζωνών ώστε να ελαχιστοποιήσουν την έκθεση σε κίνδυνο.

Ένας μεγάλος αριθμός κινήτρων οδηγεί τους ανθρώπους σε απειλές και επιθέσεις προς στα συστήματά μας. Με την εξέταση των απειλών και των κατάλληλων απαντήσεων, μπορούμε να αναπτύξουμε μια πολιτική ασφάλειας που θα ελαχιστοποιεί τον κίνδυνο που παρουσιάζεται από μια απειλή, μέσω του κατάλληλου σχεδιασμού και διαμόρφωσης της αντιπυρικής ζώνης. Αν και μια αντιπυρική ζώνη δεν μπορεί να αποτρέψει όλες τις επιθέσεις, είναι μια από τις καλύτερες μεθόδους για να προστατεύουμε τους πόρους.. Ένα άλλο σημαντικό στοιχειό που πρέπει να θυμόμαστε, είναι ότι μια αντιπυρική ζώνη δεν είναι απλά μια συσκευή. Είναι ένα σύστημα συσκευών που, εάν εφαρμόζεται κατάλληλα, παρέχει σε πολλαπλά επίπεδα μια άμυνα μεταξύ των πόρων που θέλετε να προστατεύσετε και τους κακόβουλους χρήστες που θέλουν να αποκτήσουν πρόσβαση σε αυτά.

Σε πρακτικό επίπεδο διερευνήθηκε η διαδικασία διαμόρφωσης των συσκευών ασφάλειας PIX και ASA. Για να υποστηρίξει λειτουργίες NAT, η συσκευή ασφάλειας διαχειρίζεται τα πρωτόκολλα TCP και UDP μέσω της χρήσης ενός πίνακα μεταφράσεων και ενός πίνακα σύνδεσης. Η στατική εντολή δημιουργεί μια μόνιμη μετάφραση, ενώ η χαρτογράφηση μεταξύ των τοπικών και σφαιρικών διευθύνσεων γίνεται δυναμικά με την εντολή nat. Οι δυο εντολές λειτουργούν μαζί για να κρύψουν τις εσωτερικές διευθύνσεις IP. Οι κατάλογοι έλεγχου πρόσβασης (ACL), μας επιτρέπουν να καθορίσουμε ποια συστήματα μπορούν να εγκαταστήσουν συνδέσεις, εντός η έκτος του δικτυού μας. Με τις ICMP ACL, μπορούμε να απαγορεύσουμε τα μηνύματα ping σε μια διεπαφή, ώστε η συσκευή ασφάλειάς να μην μπορεί να ανιχνευθεί στο δίκτυό.

Μέσω της ανάπτυξης υπηρεσιών AAA δείξαμε ότι μπορεί να εξασφαλιστεί η επιβολή μέτρων για να ελεγχθεί ποιος μπορεί να εισέλθει στο δίκτυο, τι δικαιώματα έχει και αν του επιτρέπεται να διαχειριστεί τη συσκευή ασφάλειας. Επιπλέον, μπορεί να γίνει καταγραφή των πληροφοριών ελέγχου χρησιμοποιώντας τις υπηρεσίες παρακολούθησης και καταγραφής. Διαπιστώθηκε επίσης ο έλεγχος της διαχειρίσεις για Telnet, SSH, κονσόλα η ASDM μέσω της επικύρωσης των αντίστοιχων συνόδων. Σε ότι αφόρα τις αποφάσεις δρομολόγησης μέσα από διάφορα σενάρια, συμπεραίνει κανείς ότι η στατική δρομολόγηση είναι κατάλληλη όταν δεν μπορεί να δημιουργηθεί

δυναμικά μια δρομολόγηση προς ένα συγκεκριμένο προορισμό. Σε μικρά και ομοιογενή δίκτυα το RIP θα αποτελούσε μια αρκετά αξιόπιστη λύση, αντίθετα σε μη στατικά και αναπτυσσόμενα περιβάλλοντα η χρήση δυναμικών πρωτοκόλλων οπός το OSPF κρίνεται απαραίτητη.

Καθημερινά, όλο και περισσότεροι οργανισμοί αναπτύσσουν σήραγγες IPSec VPN για να ενώσουν τα διαφορά δίκτυα και να μειώσουν τις δαπάνες από τις παραδοσιακές WAN συνδέσεις. Είναι ευθύνη του διαχειριστή ασφάλειας να σχεδιάσει και να εφαρμόσει μια λύση IPSec που θα ανταποκριθεί στις ανάγκες μιας οργάνωσης. Όπως παρατηρήσαμε και στο σενάριο VPN, το άλλο άκρο της σήραγγας IPSec θα πρέπει να έχει τις ίδιες ιδιότητες ISAKMP και IPSec. Εάν και πάλι η σήραγγα IPSec δεν λειτουργεί όπως αναμένεται, τότε θα πρέπει να χρησιμοποιηθούν οι κατάλληλες εντολές έλεγχου για την κατάσταση των συσχετίσεων ασφαλείας (SA).

Σαν μελλοντική εργασία αφήνεται η ανάλυση και ανάπτυξη των αντιπυρικών ζωνών που λειτουργούν σε διαφανή ή πολλαπλή εικονική κατάσταση, ο συνδυασμός ολοκληρωμένων λύσεων με συστήματα IDS/IPS και η διαμόρφωση τεχνολογιών VPN απομακρυσμένης σύνδεσης μέσω IPSEC ή SSL (WEBVPN).

Βιβλιογραφικές Αναφορές

A. A. Vladimirov, K. V. Gavrilenko, J. N. Vizulis and A. A. Mikhailovsky, “Hacking Exposed Cisco Networks: Cisco Security Secrets & Solutions”, McGraw-Hill Osborne, 2006.

A. Carasik-Henmi, T. W. Shinder, C. Amon, R. J. Shimonski, D. L. Shinder, “Best damn firewall book period”, Syngress Publishing, 2003.

A. Henmi, M. Lucas, A. Singh, C. Cantrell, “Firewall Policies and VPN Configurations”, Syngress Publishing, 2006.

A. Whitaker, D. P. Newman, “Penetration Testing and Network Defense”, Cisco Press, 2005.

C. Anley, J. Heasman, F. Linder, G. Richarte, “The Shellcoders Handbook” Wiley Publishing, 2007.

C. Riley, U. Khan, M. Sweeney, “Cisco PIX Firewalls: Configure, Manage, & Troubleshoot”, Syngress Publishing, 2005.

R. Deal, “Securing Networks with PIX and ASA SNPA Student Guide v4.0”, 2005.

E. Zwicky, S. Cooper, D. B. Chapman, D. Russell, “Building Internet Firewalls (2nd Edition)”, O’Reilly, 2000.

G. Abelar, “Securing Your Business with Cisco ASA and PIX Firewalls” Cisco Press, 2005.

G. Bastien, C. Degu, “CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide”, Cisco Press, 2003.

G. De Laet, G. Schauwers, “Network Security Fundamentals”, Cisco Press, 2004.

G. Schudel, D. J. Smith, “Router Security Strategies: Securing IP Network Traffic Planes” Cisco Press, 2008.

I. Pepelnjak, “Deploying Zone-Based Firewalls”, Digital Shortcut, 2007.

J. Frahim, O. Santos, “Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance”, Cisco Press, 2005.

M. Gibbs, G Bastien, E Carter, C Abera, “CCSP SNPA Official Exam Certification Guide, Third Edition”, Cisco Press, 2006.

M. Lynn, “Cisco IOS Shellcode and Exploitation Techniques”, Internet Security Systems, 2006.

R. Lusignan, O. Steudler, J. Allison, “Managing Cisco Network Security”, Syngress Publishing, 2000.

R. Stephens, B. J. Stiefel, S. Watkins, S. Desmeules “Configuring Check Point NGX VPN-1/FireWall-1”, Syngress Publishing, 2005.

R. Tibbs, E. Oakes, “Firewalls and VPNs: Principles and Practices” Prentice Hall, 2005.

S. Manzuik, A. Gold, C. Gatford, “Network Security Assessment”, Syngress Publishing, 2006.

S. Northcutt, K. Frederick, S. Winters, L. Zeltser, R. W. Ritchey , “Inside Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems” Sans Giac, 2002.

W. Noonan, I. Dubrawsky, “Firewall Fundamentals”, Cisco Press, 2006.

W. R. Cheswick, S. M. Bellovin, D. Rubin, “Firewalls and Internet Security: Repelling the Wily Hacker (2nd Edition)”, Addison-Wesley Professional Computing Series, 2003.